Power and EM Attacks on Passive 13.56 MHz RFID Devices

Michael Hutter[1], Stefan Mangard[2], Martin Feldhofer[1]

CHES 2007

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

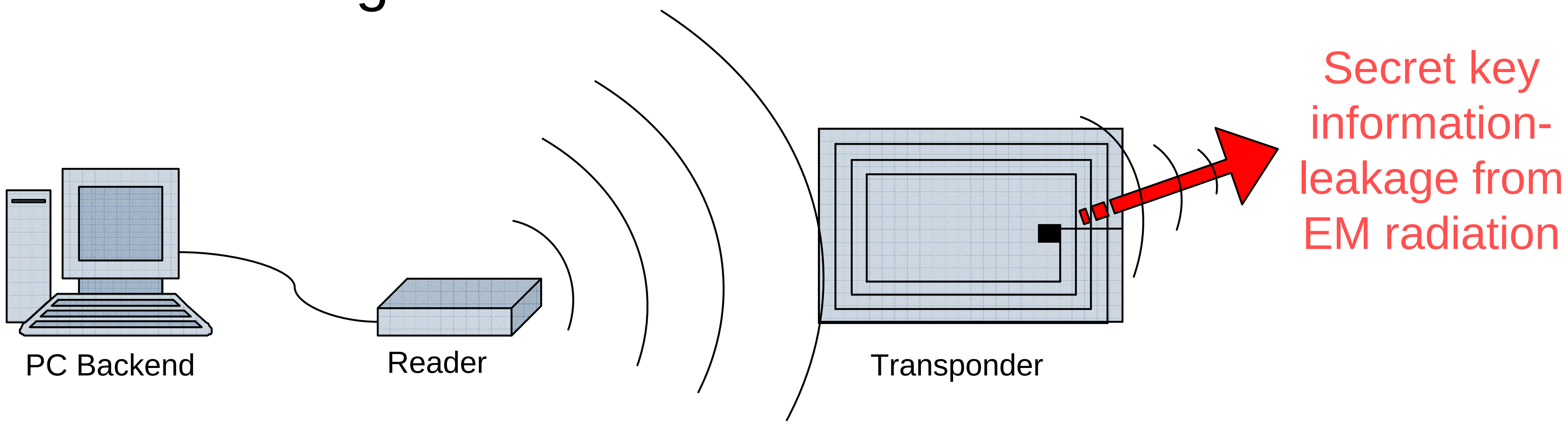
[2]Infineon Technologies AG, Security Innovation

Presentation Outline

- Introduction
- RFID prototype devices
- Measurement setups
- Results
- Conclusions and future work

Introduction

- RFID (Radio Frequency Identification)
- Air interface
  - Power supply
  - Communication
  - Clock signal



Side-Channel Attacks on RFID

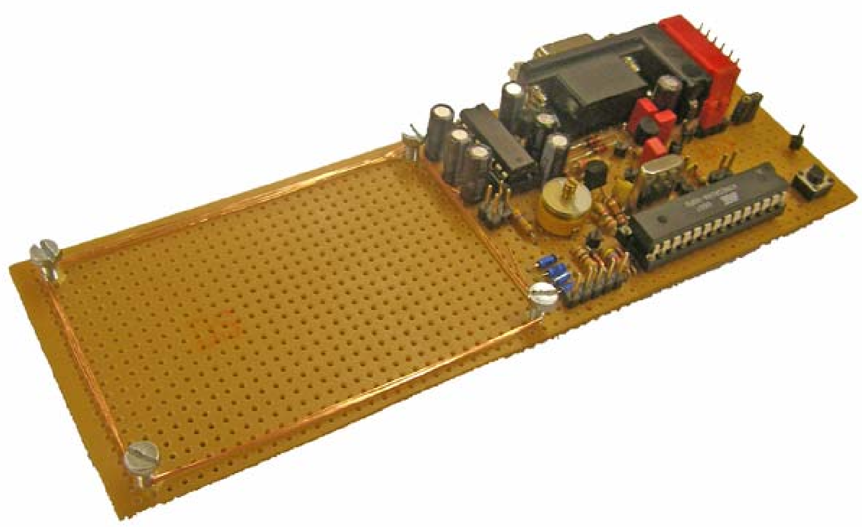
- Conventional DPA
  - Problem: No power supply contacts available
- EM analysis
  - Problem: Strong RF field of the reader superposes all interesting chip emissions
- Challenge:
  - Circumvent the interfering reader signal through filtering or signal-cancellation techniques

Side-Channel Analysis

- Side-channel analysis of two different RFID prototype devices
  - Prototype with a microcontroller (software AES)
  - Prototype with an AES coprocessor (hardware AES)

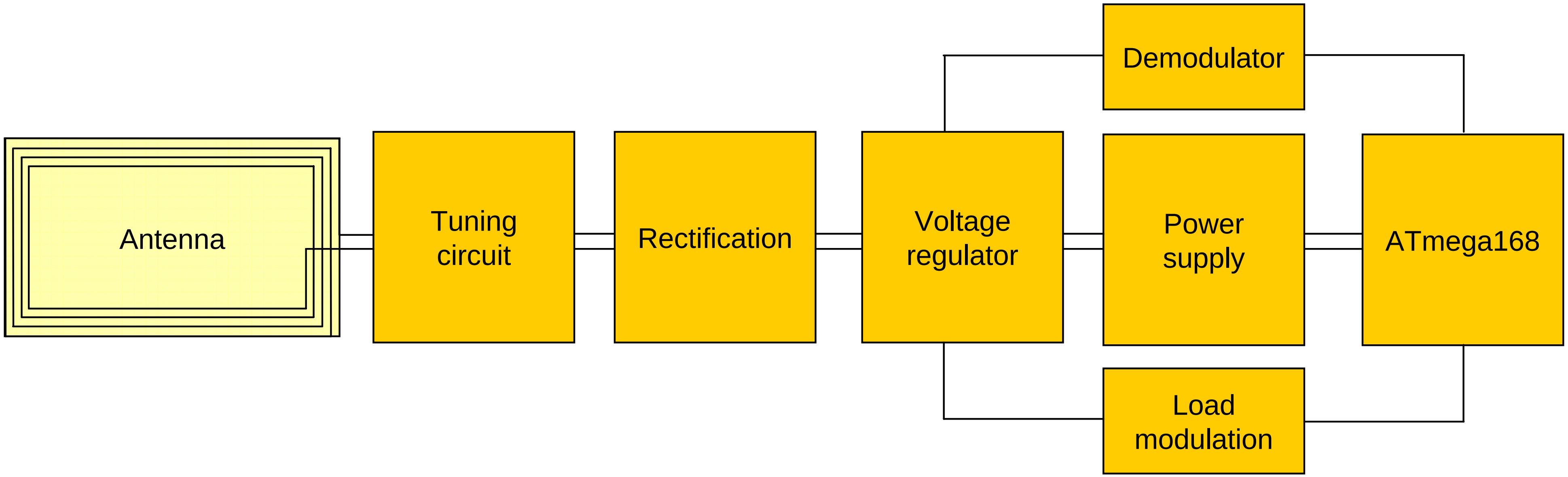
RFID Prototype with a Microcontroller

- Passive RFID tag
- Low-power design
- ISO-15693
- Software AES is used in a challenge-response protocol



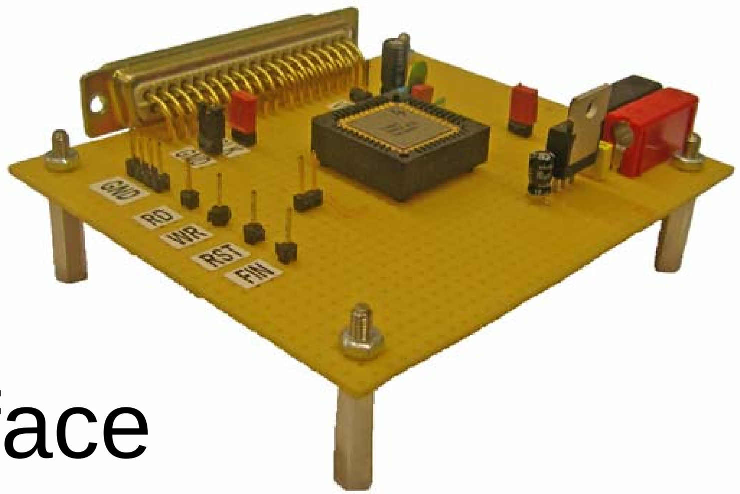
Block Diagram

- Antenna
  - ISO-7810, four windings
- Analog front-end



RFID Prototype with AES Coprocessor

- Small AES hardware implementation
  - 0.25 mm^2 chip die-size
  - 0.35 µm CMOS process
- Low power
  - ~3 µA of current @ 100 kHz
- 8-bit microcontroller interface
- Controlled via an FPGA board
- Passively powered using an additional RFID antenna



RFID Prototype vs. Single-Chip Tag

- Larger parasitic antennas
- Analog front-end and digital chip on the same die
- Low-power consumption
- Clock synchronization
- Trigger signal

Measurement Setups Overview

- Resistor
- EM probes
- EM probes and a receiver
- Helmholtz arrangement

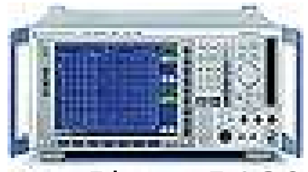
Power Measurement Setups (1)

- Resistor
  - Traditional power measurement
  - Placed between the analog front-end and the digital circuit
  - Used as a reference attack

- EM probes
  - Bandwidth: 0 – 50 MHz and 30 – 3000 MHz
  - Positioning: directly upon the chip (parallel to the chip layer)

Power Measurement Setups (2)

- EM probe and a receiver
  - Spectrum analyzer (*ESPI R&S)*
  - Connected to the oscilloscope
  - Used to filter and amplify emitted frequency bands

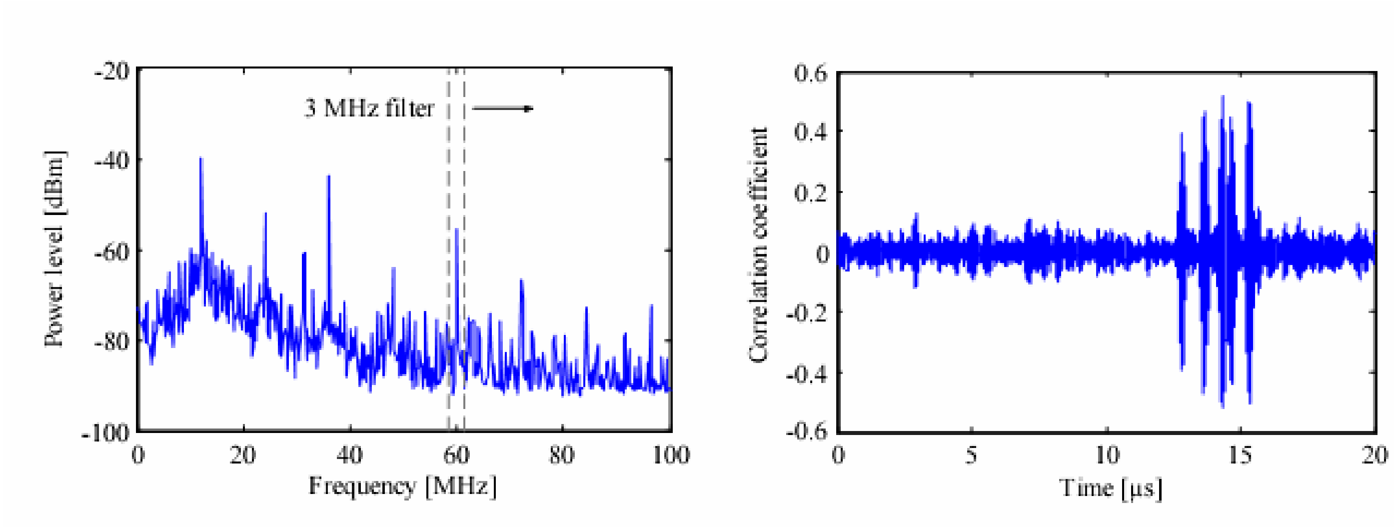


Picture R&S®

- Helmholtz arrangement
  - Specified in the ISO-10373-6 standard
  - Normally used for compliance testing
  - Reader coil and two sense coils
  - Carrier attenuation of 40dB

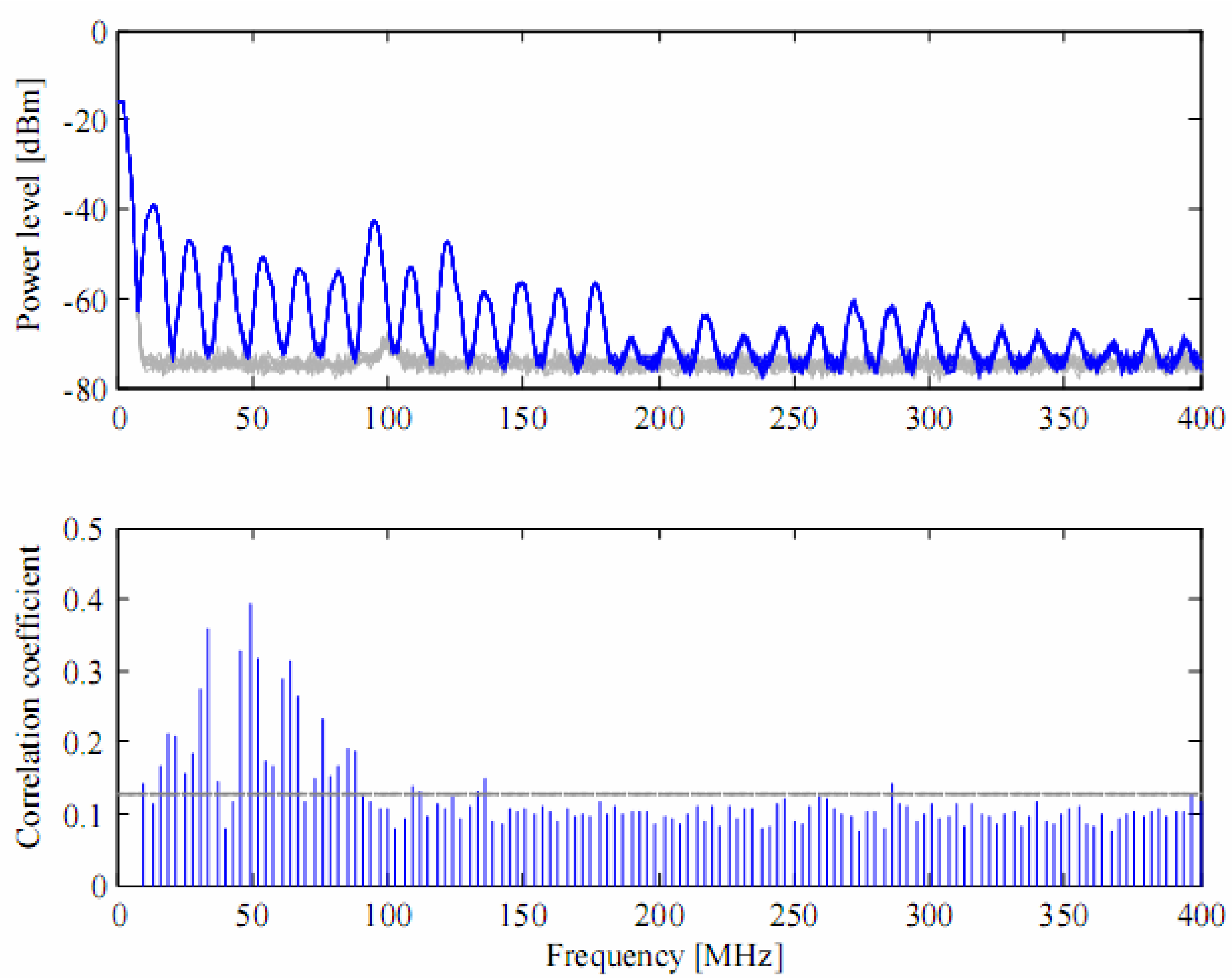
Filtering Data-Dependent Emissions

- Find the highest data-dependent frequency in the EM spectrum
- Apply the filter inside the reader field

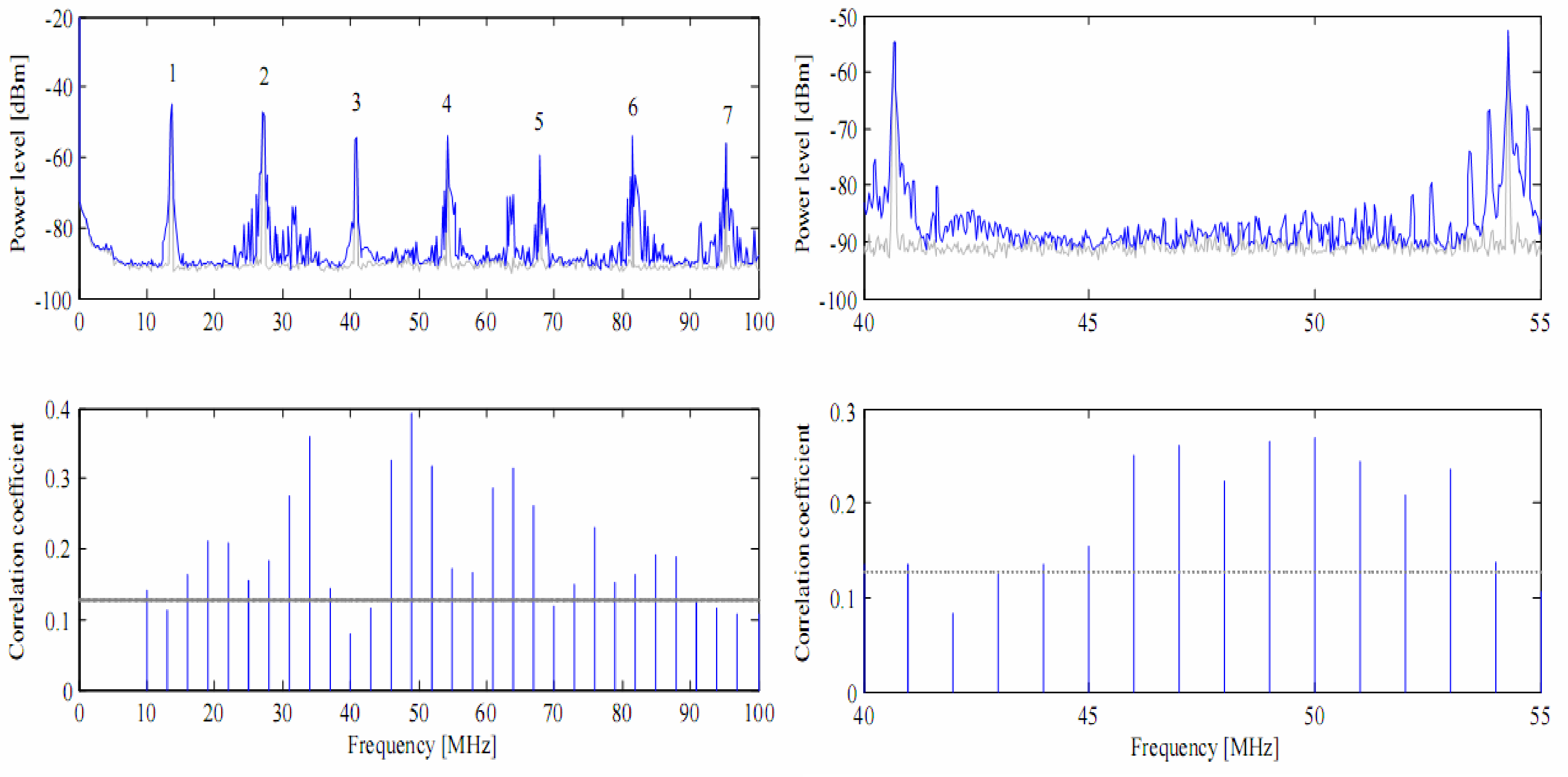


- Filter bandwidths of 10 MHz, 3 MHz, 1 MHz and 1 kHz used
- 1000 traces have been captured on each frequency band

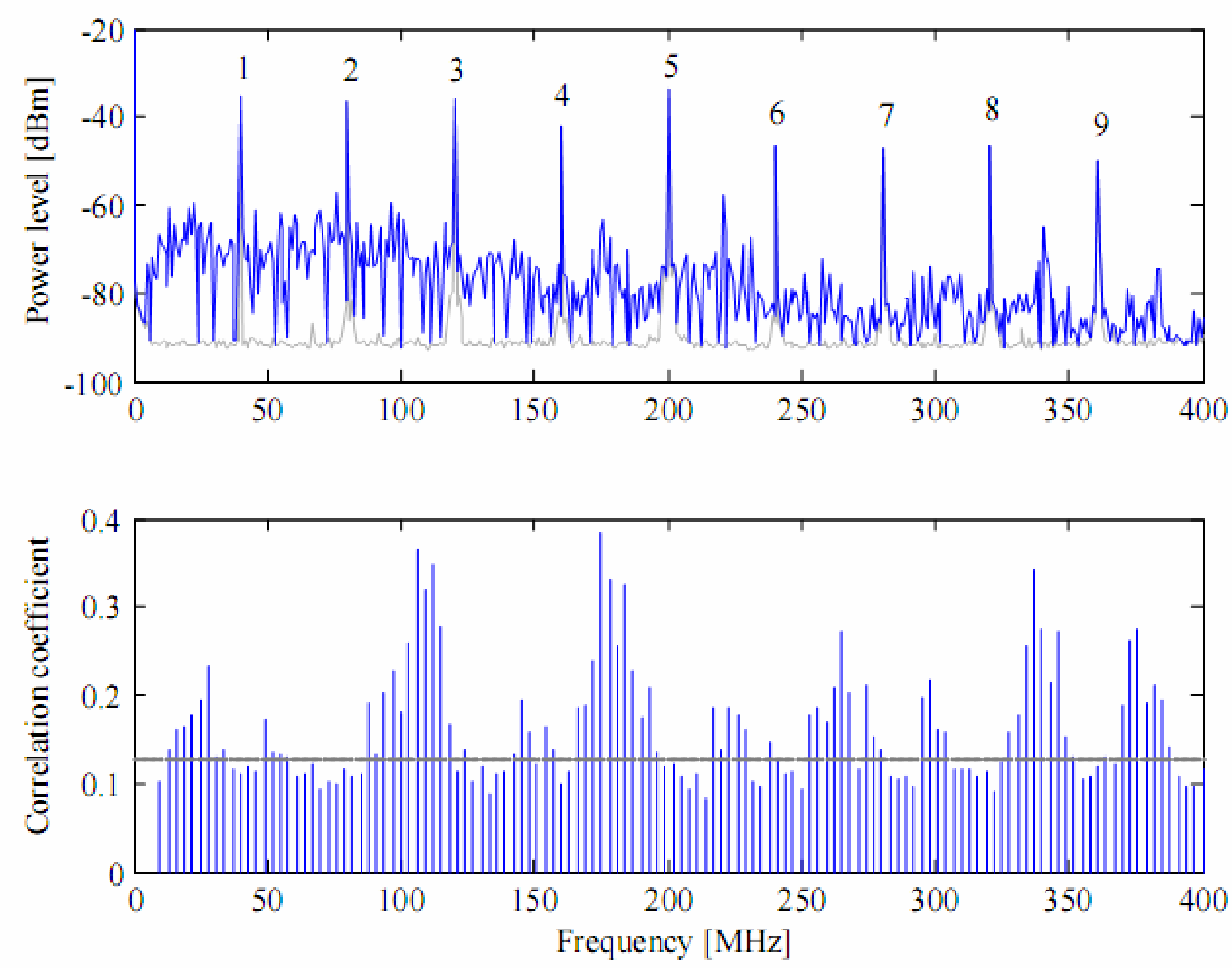
Side-Channel Leakage across the EM Spectrum of the RFID Prototype with a Microcontroller



Zoom into the Spectrum



Side-Channel Leakage across the EM Spectrum of the RFID Prototype with an AES Coprocessor



Performed Attacks

- Power and EM
- Helmholtz arrangement
- Attacking Scenarios
  - Actively and passively powered
  - Placed inside and outside the RF field of the reader
- 10,000 traces have been recorded
- Hamming-weight model
- Target: first S-box output in round one of AES

Results

	DPA		DEMA		Helmholtz
	Actively powered	Passively powered	Actively powered	Passively powered	Passively powered
	Outside	Inside	Outside	Inside	Inside
Micro-controller	0.64 (~50)	0.67 (~45)	0.73 (~35)	0.19 (~770)	0.06 (~7700)
AES coprocessor	0.39 (~170)	0.17 (~970)	0.34 (~225)	0.15 (~1200)	N/A

Conclusions and Future Work

- Contact-less devices are as vulnerable as contact-based devices
- Attacks can be further improved
  - Increasing the SNR of the measurement setup
  - Advanced filtering
  - Improved reader-field cancellation techniques
- Characterization of data-dependent frequency emissions

Side-Channel Analysis Lab

Michael.Hutter@iaik.tugraz.at

Stefan.Mangard@infineon.com

Martin.Feldhofer@iaik.tugraz.at

http://www.iaik.tugraz.at/research/sca-lab