ChameleonMini

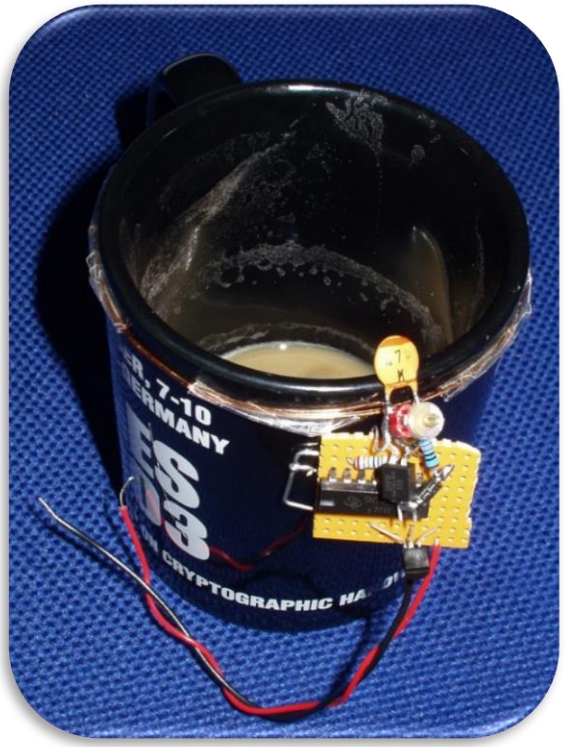
A Multifunctional RFID/NFC Tool

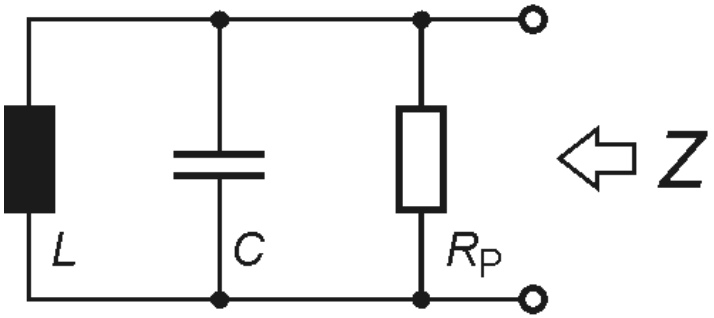
A Bit of History

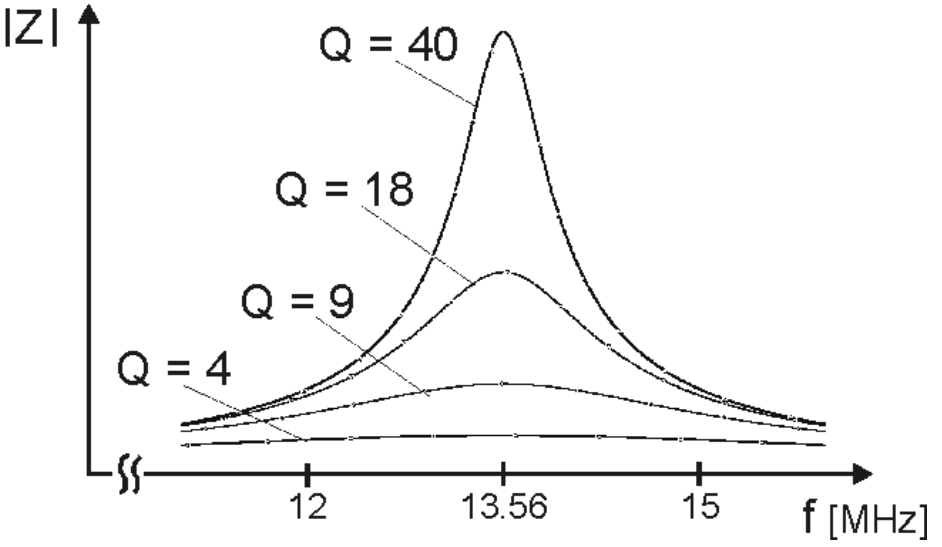
2006: Coffee Cup Tag Emulator

2006: Coffee Cup Tag Emulator

1. Antenna Design

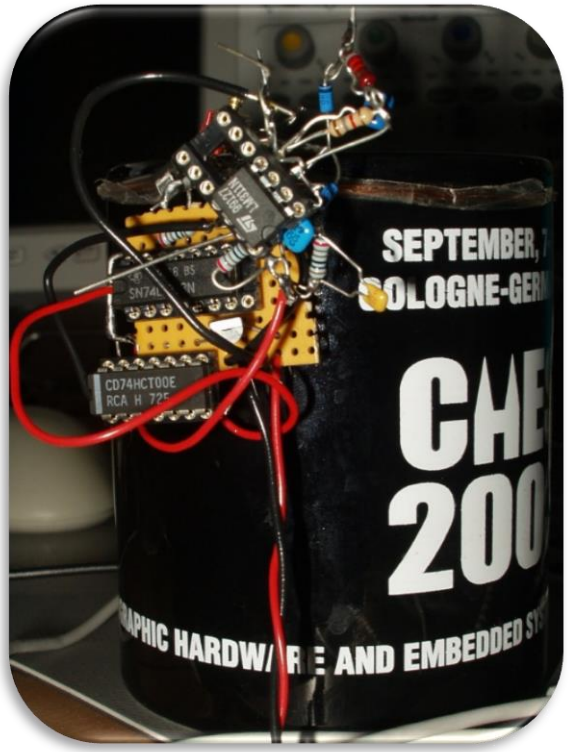


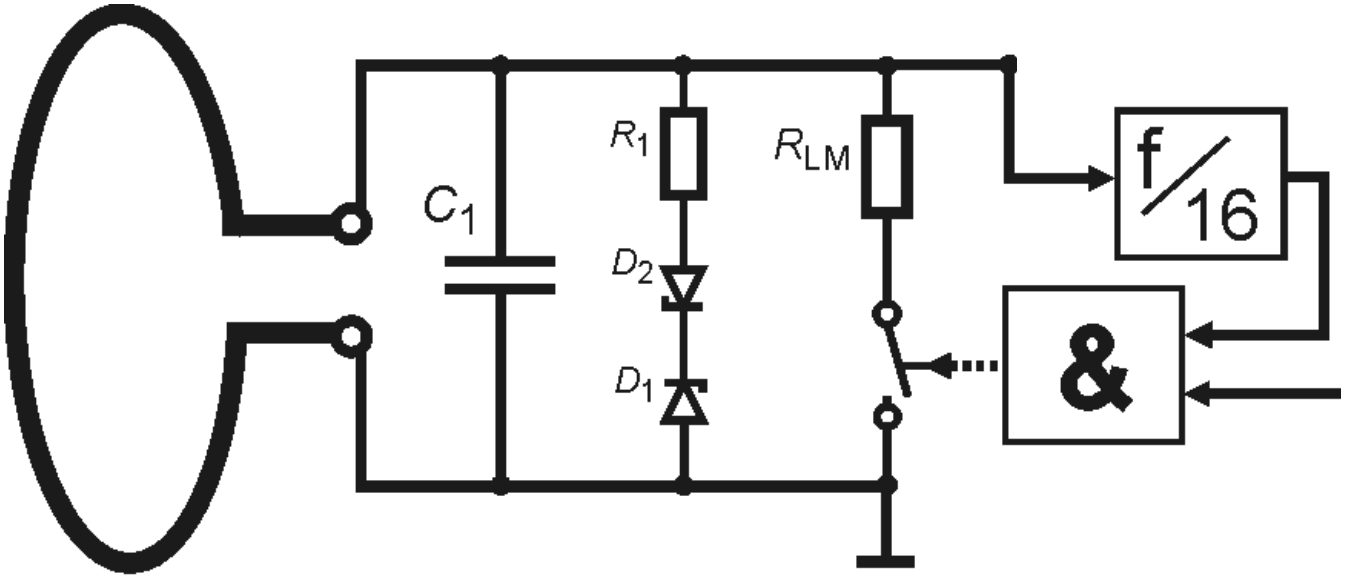




2006: Coffee Cup Tag Emulator

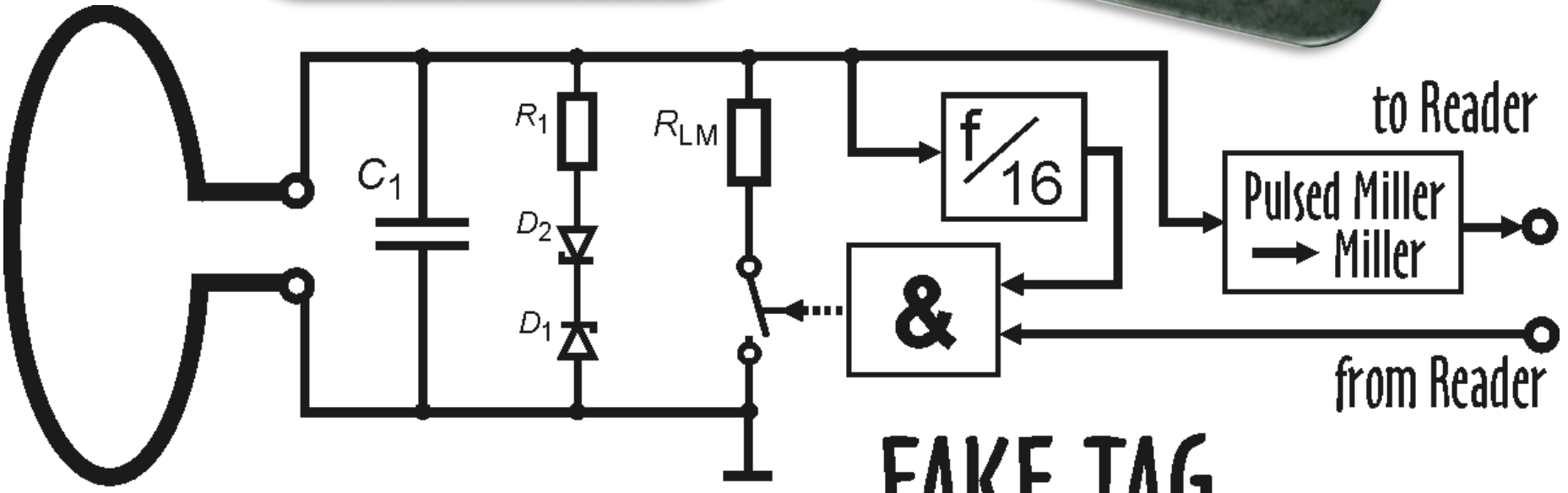
2. Load Modulation





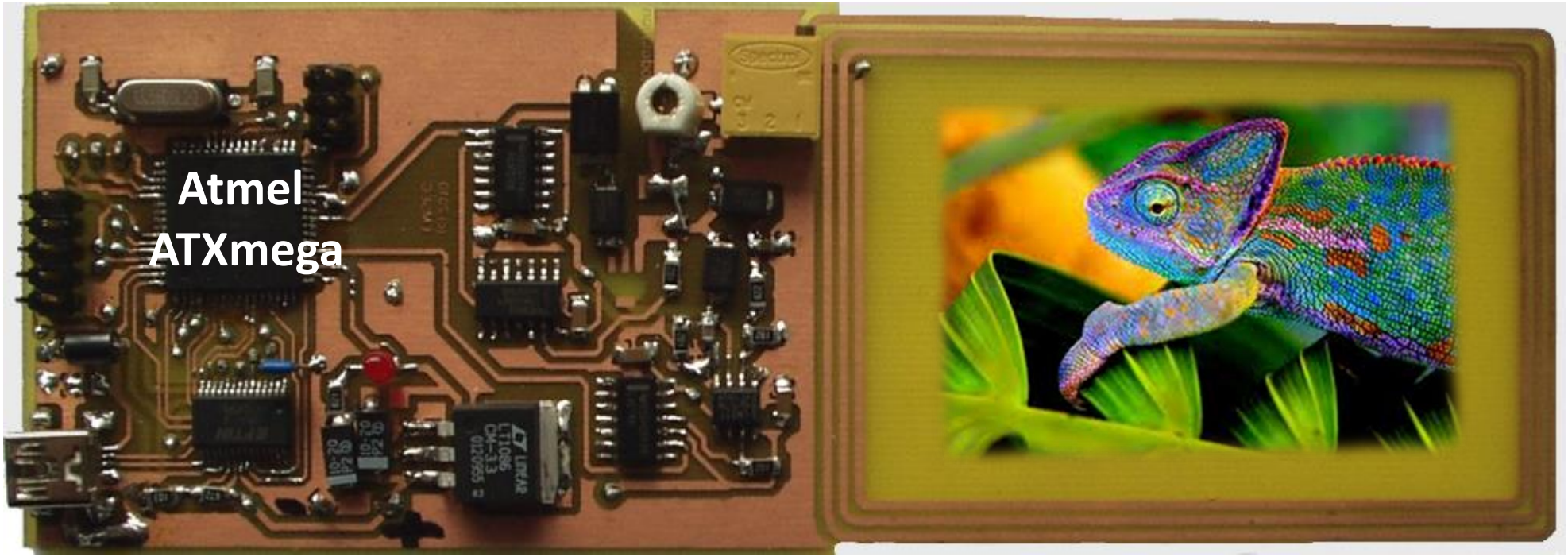
2007: Fake Tag

KASPER OSWALD



2010: The Primal-Chameleon

A Versatile Emulator for Contactless Smartcards

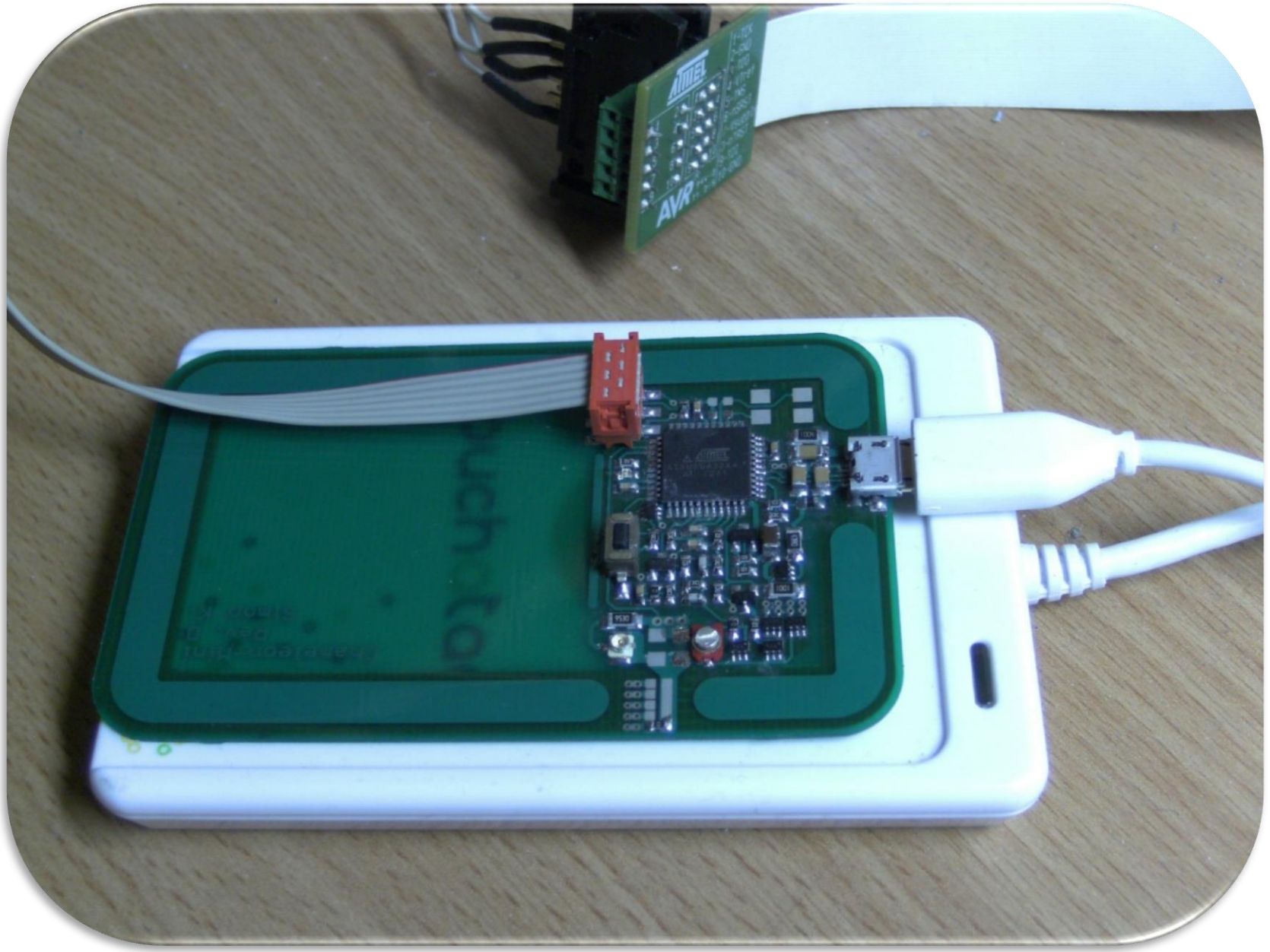


- Mifare Classic: **Crypto1** stream cipher
- Mifare DESFire *MF3ICD40*: Auth. with **(3)DES**
- Mifare DESFire EV1: Auth. with **AES-128**, **(3)DES**
- … and other ISO14443 / ISO15693 cards

ChameleonMini

KASPER OSWALD

2013: Rev.D

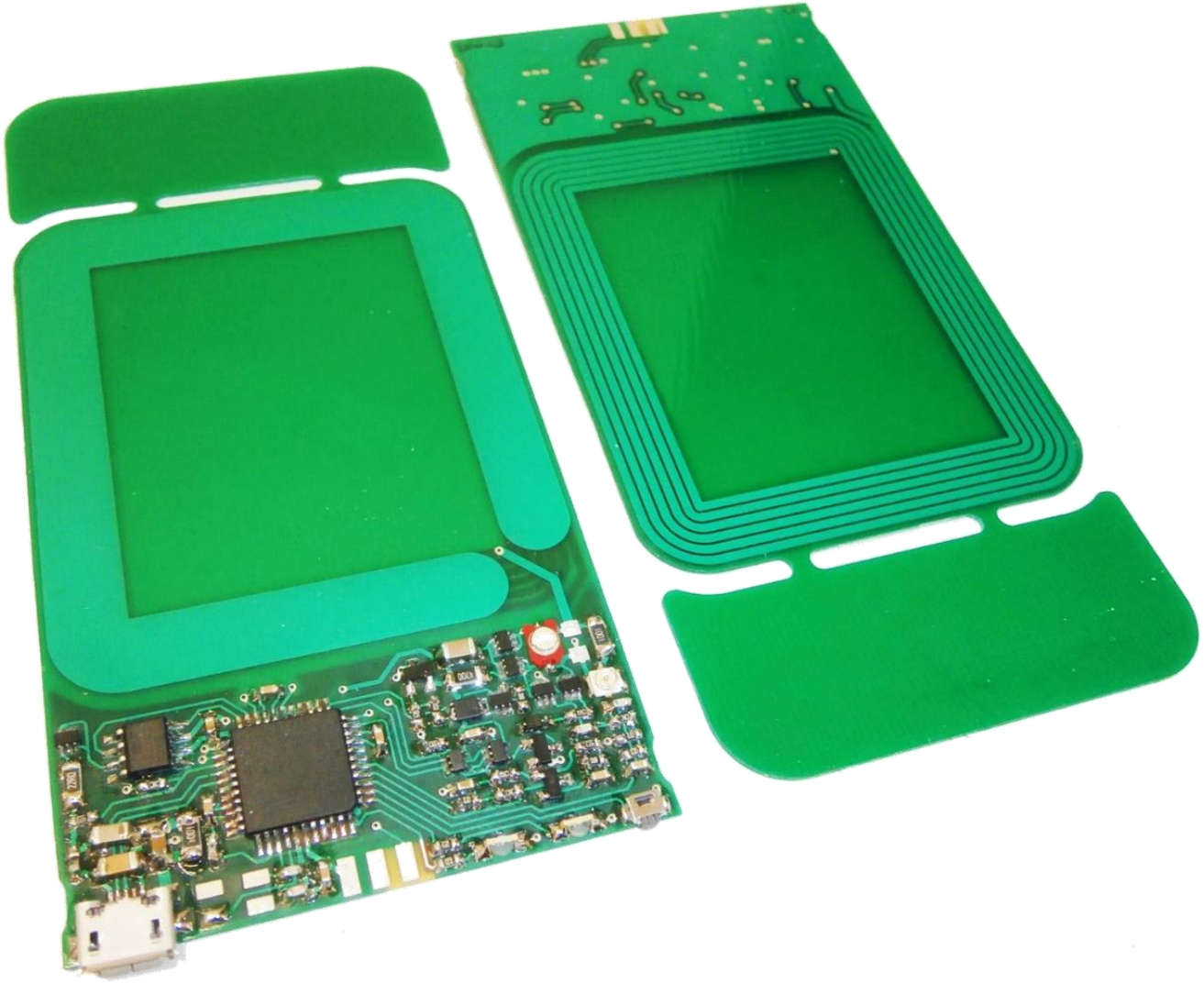


ChameleonMini

KASPER OSWALD

2014: Rev.E

- 8 card slots
- Breakable antenna
- Improved USB command set
- Widespread

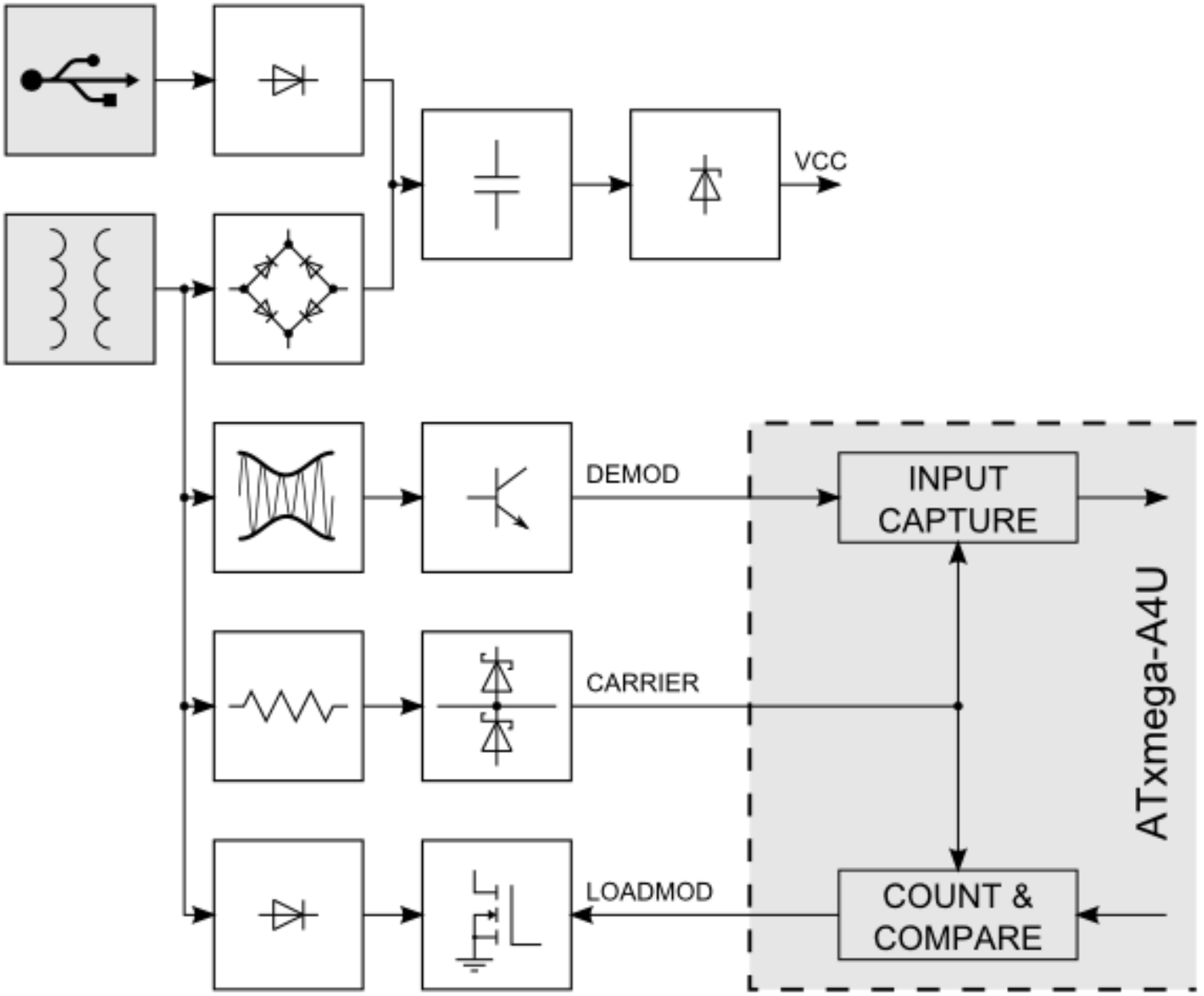


open source project: **https://github.com/emsec/ChameleonMini**

ChameleonMini Rev.E

KASPER OSWALD

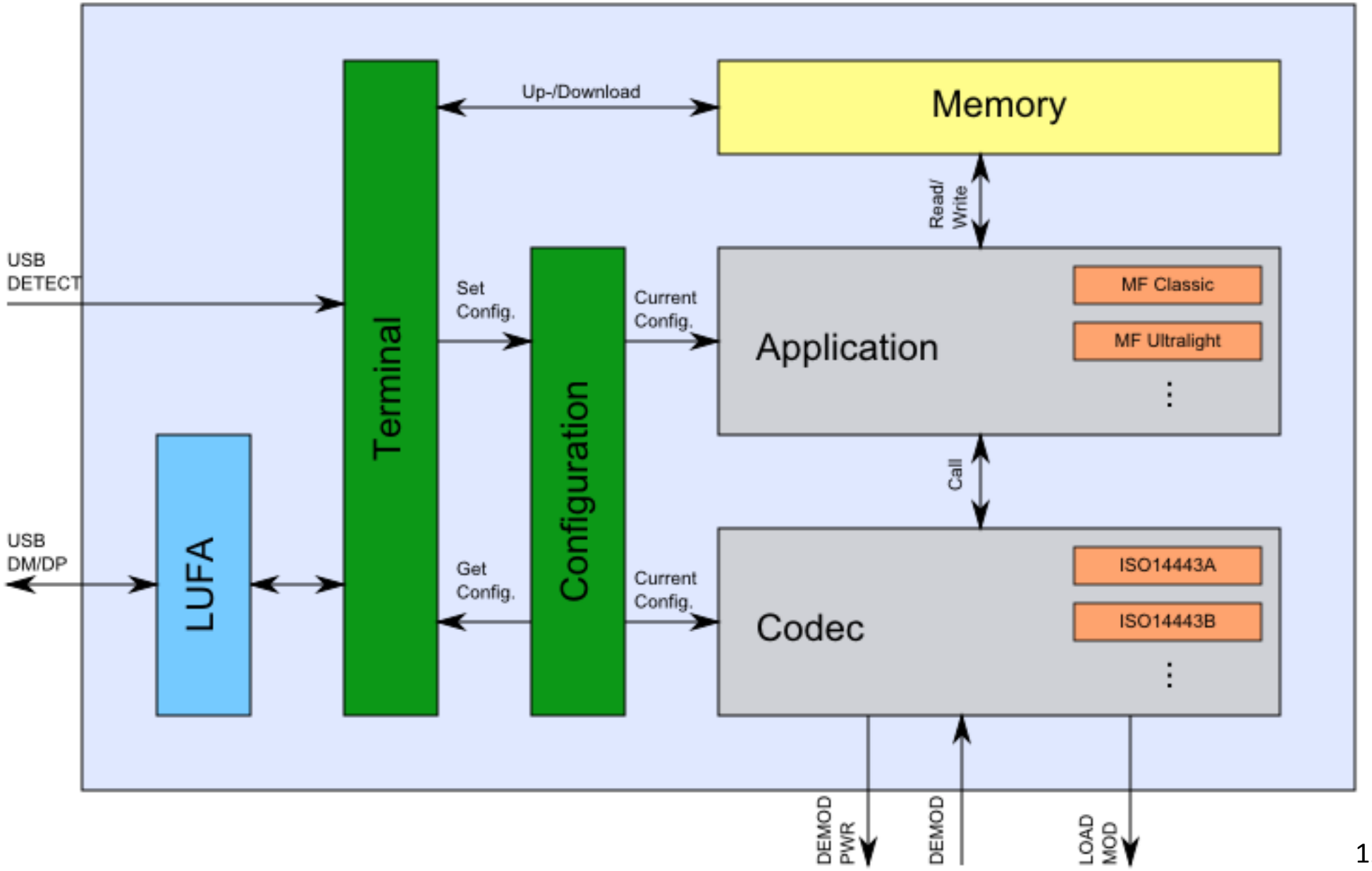
Block Diagram of Hardware



ChameleonMini Rev.E

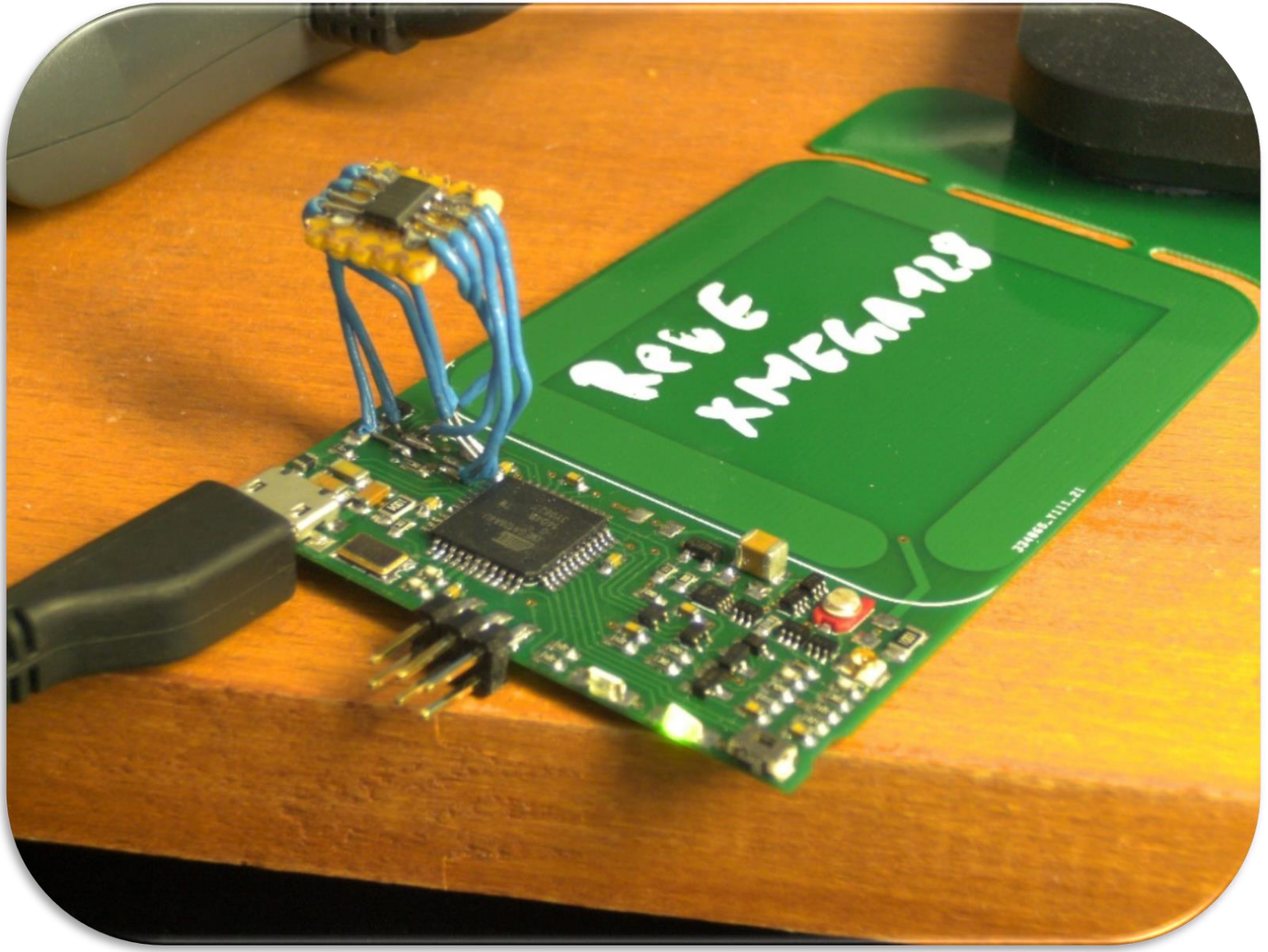
KASPER OSWALD

Block Diagram of Firmware



Rev.E is not enough…

Testing FRAM and ATXMega128A4U



ChameleonMini

Rev. F

- FRAM
- Li-Ion Battery
- **(Basic) RFID Reader**
- ISO 14443/15693
- Sniffing
- Log Mode

ChameleonMini Rev.F

KASPER OSWALD

Log Mode / Sniffing

- Emulation: monitor RFID reader and Chameleon
- Sniffing: Chameleon is „invisible“ during recording
- Precise time stamps
- Live logging

Some ChameleonMini Use Cases

- Virtual wallet with up to eight cards
- User-definable token for access control
  → upgrade of (cryptographic) algorithms possible
- Compliance tests (in fab)
- Functional tests with NFC door lock systems
- Pentesting/Fuzzing of RFID/NFC Readers:
  send unexpected data → buffer overflow, …
- Power-switch: effective privacy protection/
  Relay-attack countermeasure (user interaction)
- Research / teaching (RFID / NFC / lightweight crypto)
- ….

ChameleonMini as a Flight Recorder

1. System in test mode

(everything is allowed)

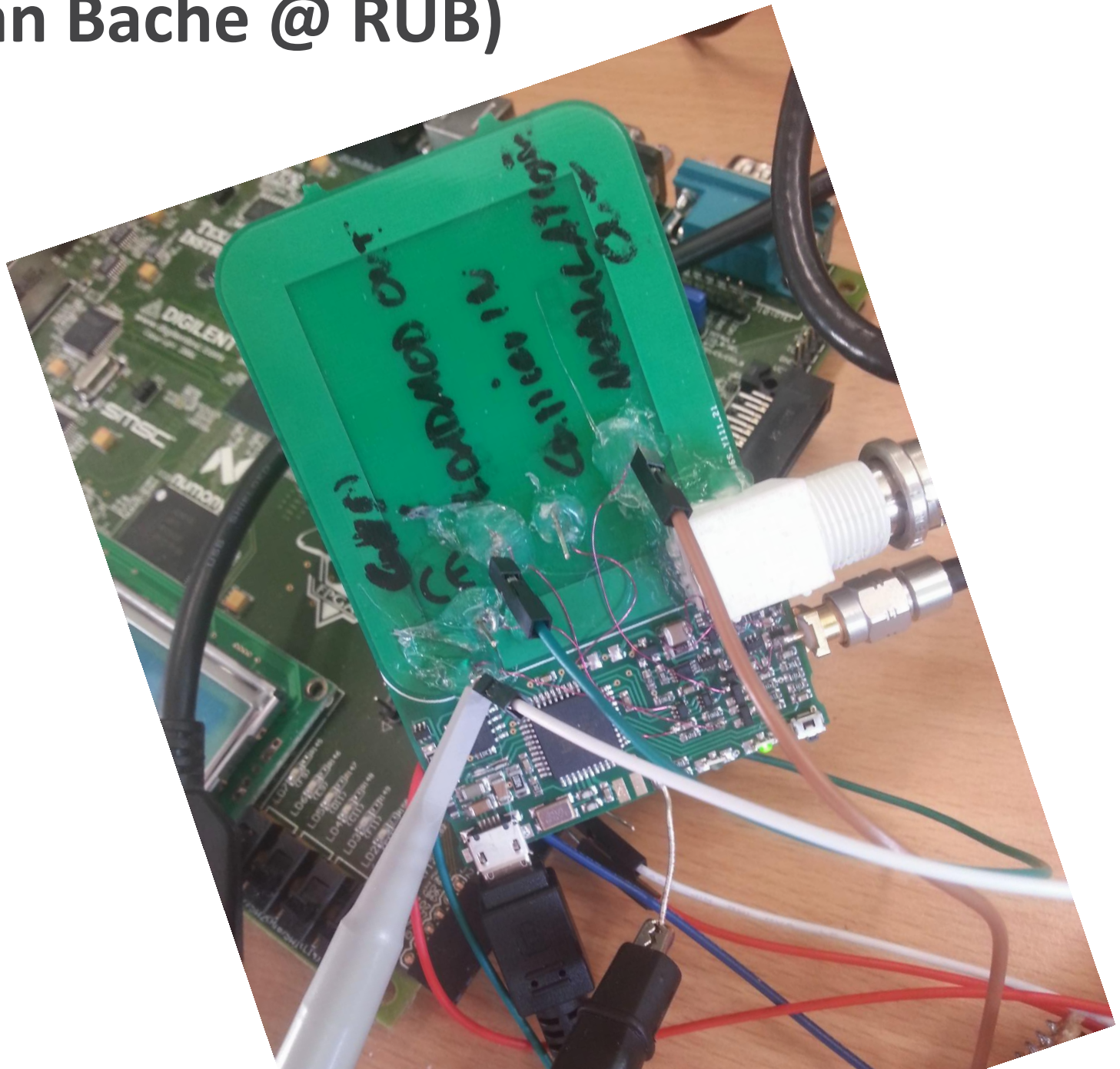
- Record and analyze **all** communication
- Distinguish normal behavior / attacks / bugs / user errors

2. Block all unwanted actions

3. System in „normal operation“ mode

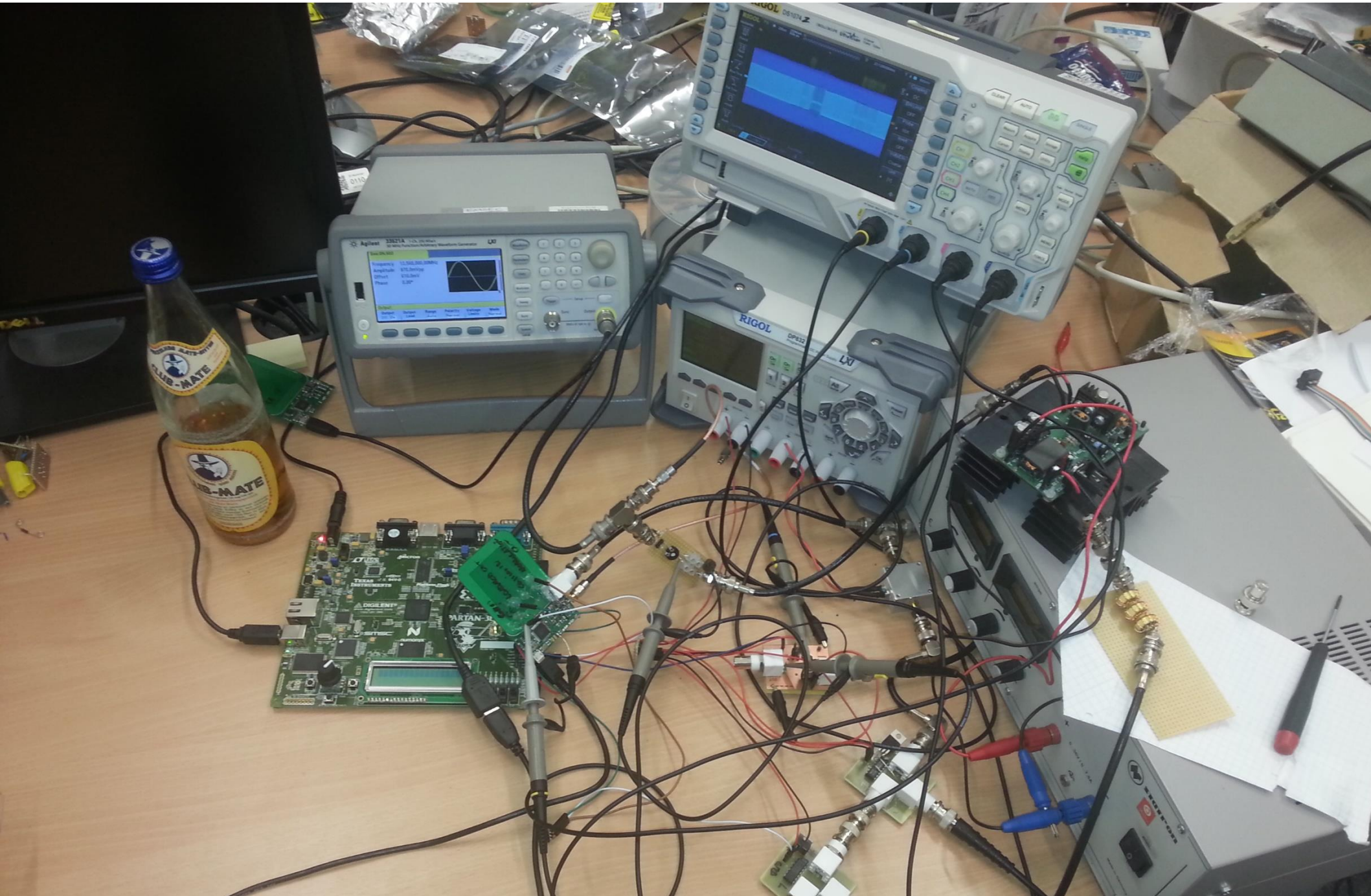
→ Keep track of further errors and react

Creative Usage of ChameleonMini (Florian Bache @ RUB)



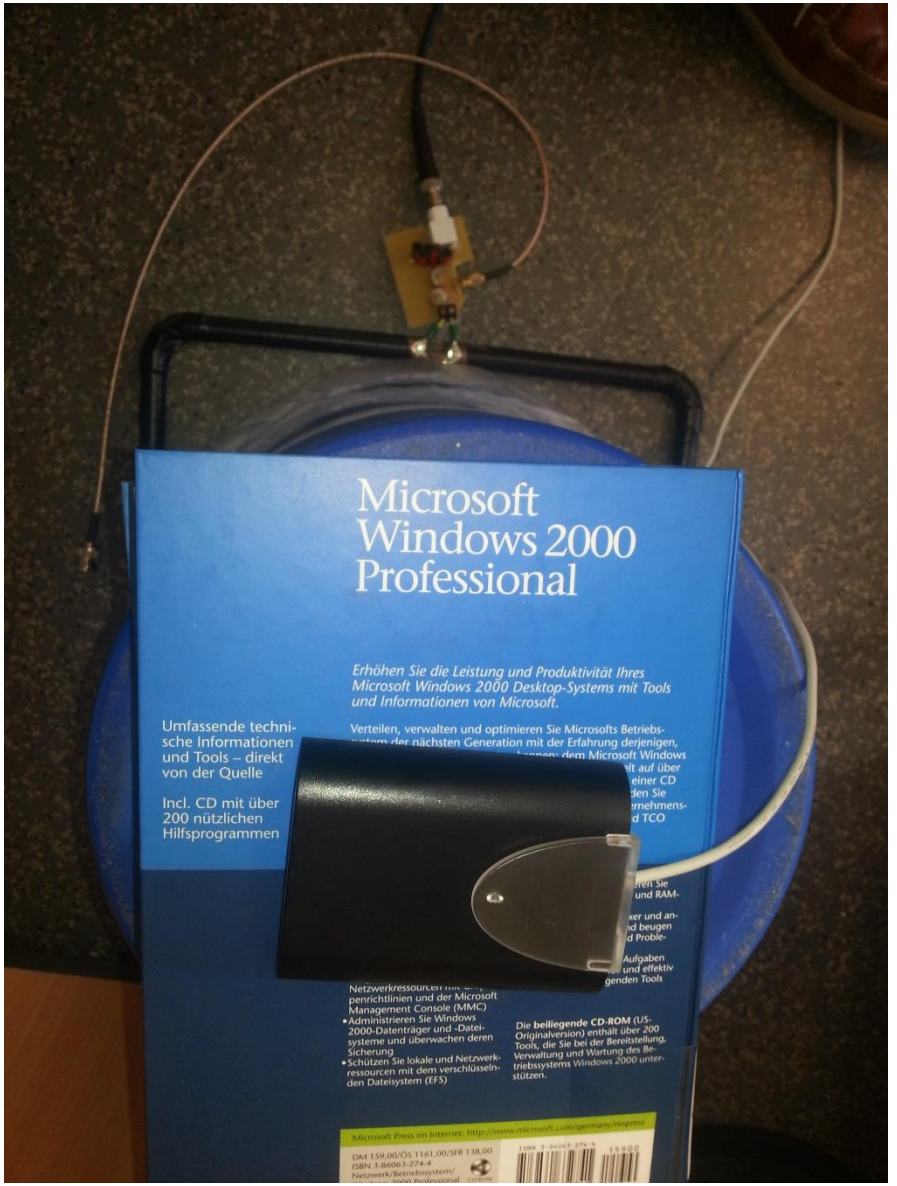
Long Range ISO14443 Contactless Card

KASPER OSWALD



A Useful Book:

(NFC Tag Range Extension: more than 70cm)



Thanks for supporting the ChameleonMini project!