RUB

RUHR-UNIVERSITÄT BOCHUM

FPGA-based Implementation Attacks with GIAnT

9th CryptArchi Workshop, Bochum

June 17th, 2011

David Oswald, Timo Kasper, Stephen Markhoff, Christof Paar
Chair for Embedded Security, Ruhr-University Bochum

hgi
Horst-Görtz Institut
für IT Sicherheit

EMSEC
EmbeddedSecurity

Acknowledgements

- **Timo Kasper**
- **Stephen Markhoff**
- **Christof Paar**

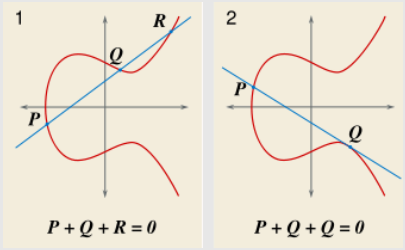
Outline of this talk

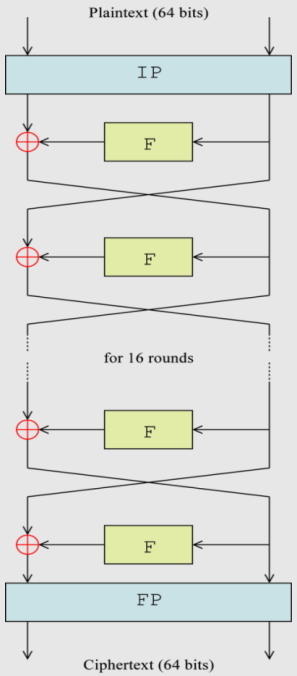
- Motivation
- GIAnT: Architecture and Features
- Practical Results
  - RSA-CRT on ATMega
  - 3DES on ATXMega
- Live Demo
- Conclusion

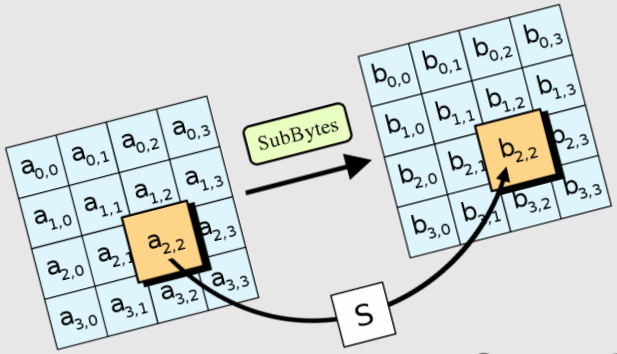
Motivation

Modern Cryptography

- E.g. AES, 3DES, RSA, ECC, …
- Mathematically secure
  ⇒ **No analytical attacks**
- Large key size
  ⇒ **No brute-force attacks**
- All problems solved?
- **No!** Crypto has to be implemented somewhere



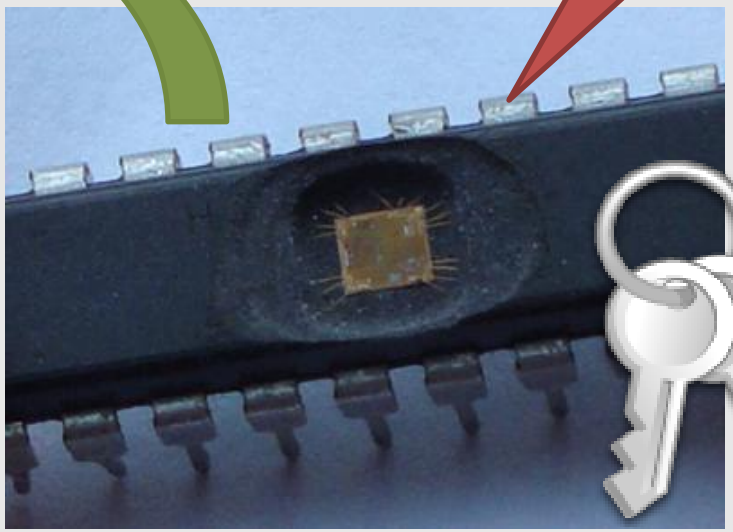




Source: Wikipedia

Implementation Attacks

Side-Channel Analysis



Cryptographic IC

Fault injection

Off-the-shelf Equipment

- Digital Oscilloscope: **2000 – 50000 USD**

- Signal Generator: **2000 – 10000 USD**

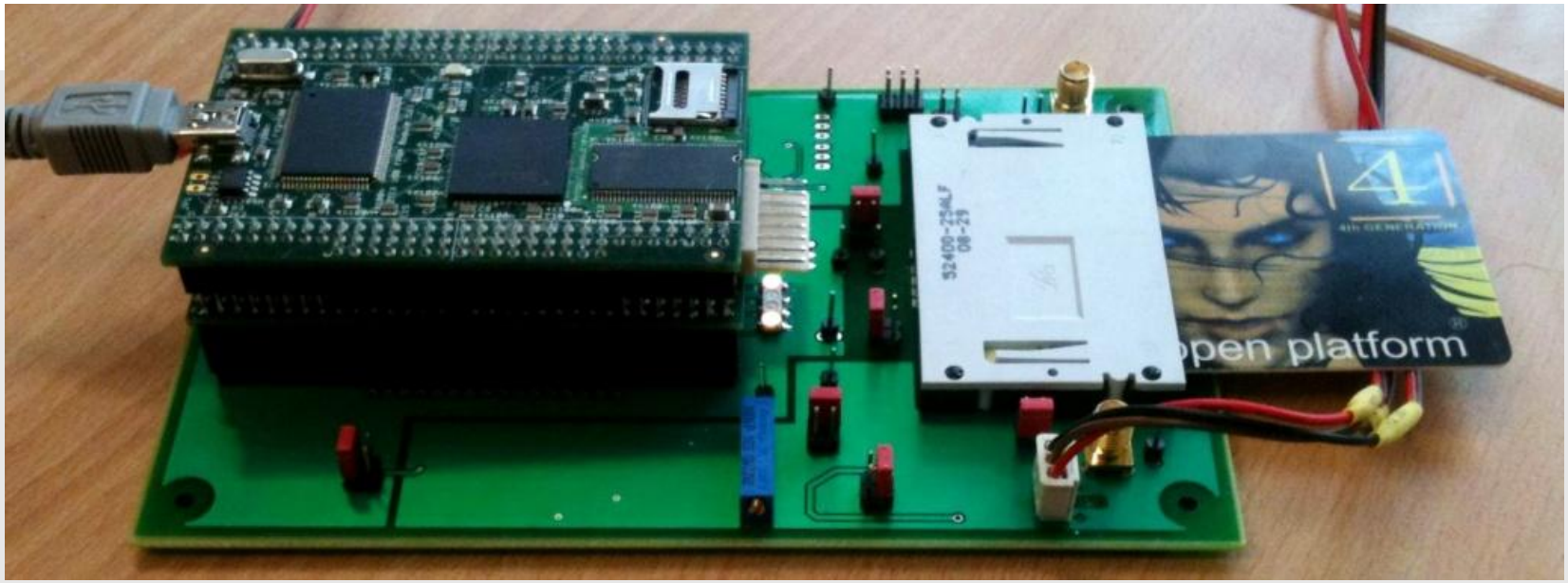
- Specialized Devices:
  - E.g. by Riscure

Sources: LeCroy, Agilent, Riscure

- **Expensive**
- Usually **not fully open / extendable**

Our contribution: The GIAnT

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald



- **G**eneric **I**mplementation **An**alysis **T**oolkit
- **Low-cost**: < 300 USD
- ZTEX Spartan6 FPGA module
- **Open-source**: sf.net/projects/giant
- Support for fault injection and side-channel analysis

RUHR-UNIVERSITÄT BOCHUM

RUB

Architecture and Features

GIAnT

Typical Setup: Overview

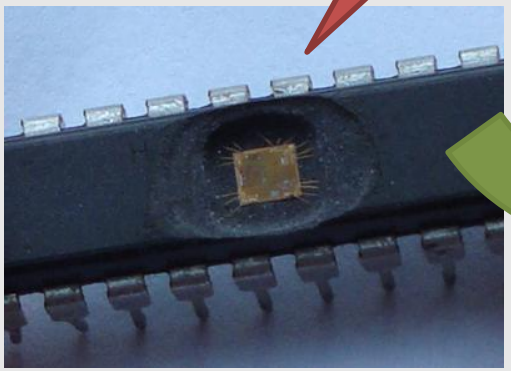
Controlling PC

Control (USB)

GIAnT: ZTEX FPGA module + custom board

Power supply

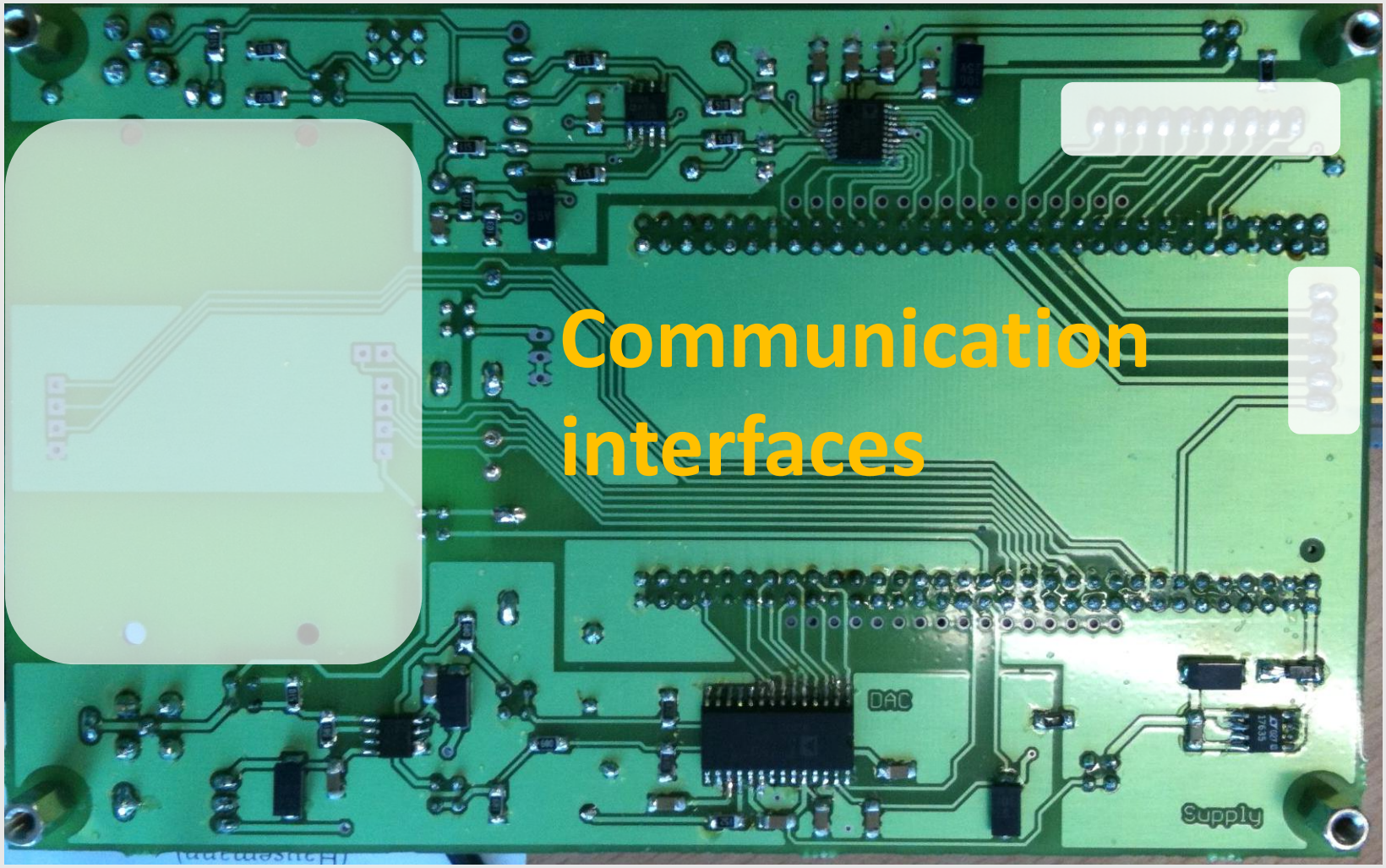
Communication



Device under test

Power consumption

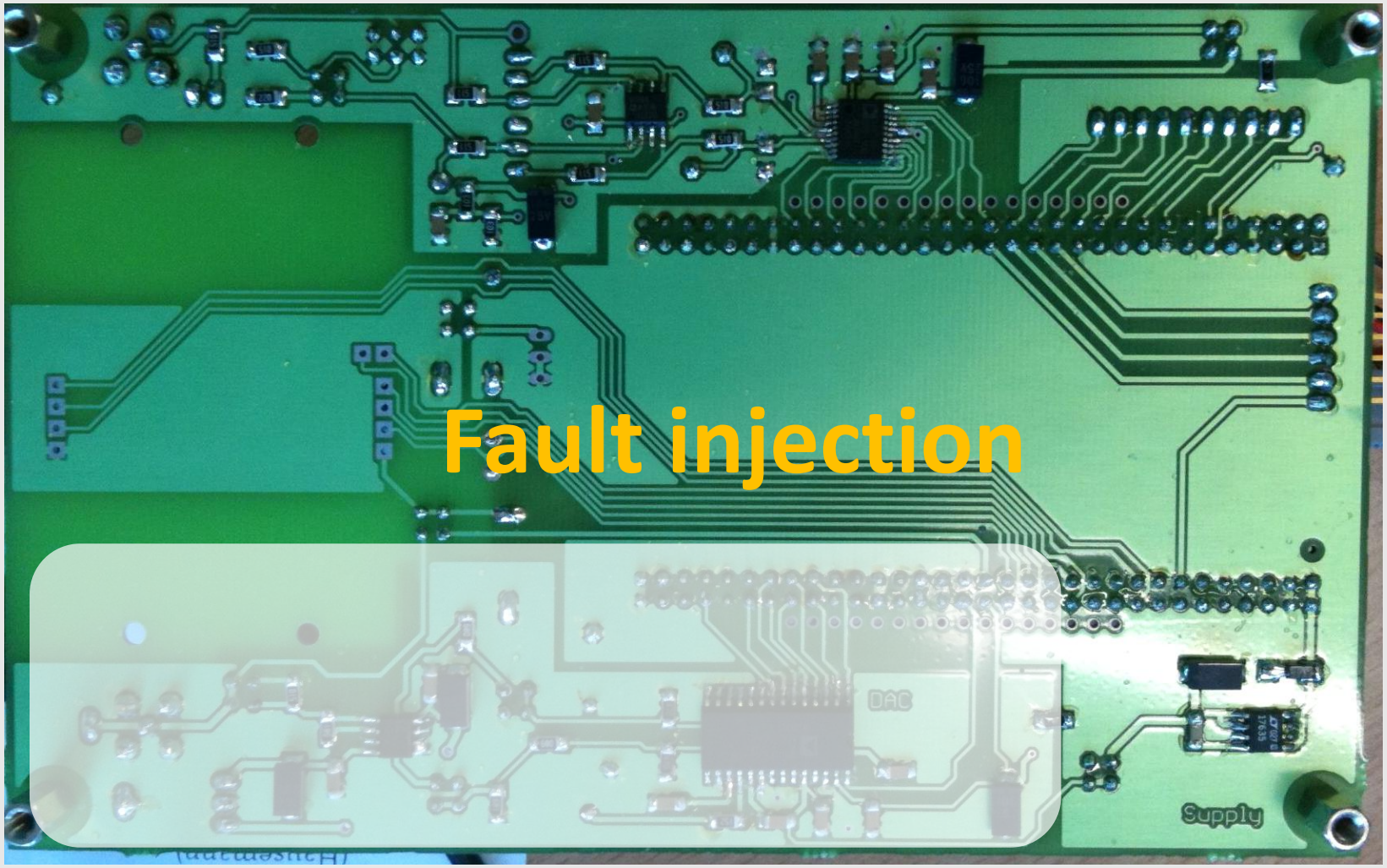
GIAnT: Hardware Overview



Communication Interfaces

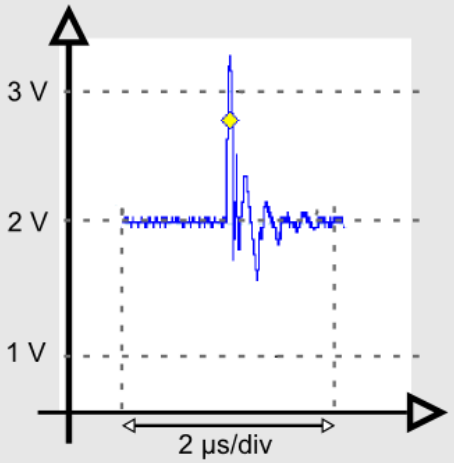
- Controlled and programmed via USB 2.0
- Interfaces to DUT
  - General-purpose I/O
  - Serial links (SPI, TWI, …)
  - ISO 7816 (Contact-based smartcards)
  - ISO 14443 (Contactless smartcards)
  - …

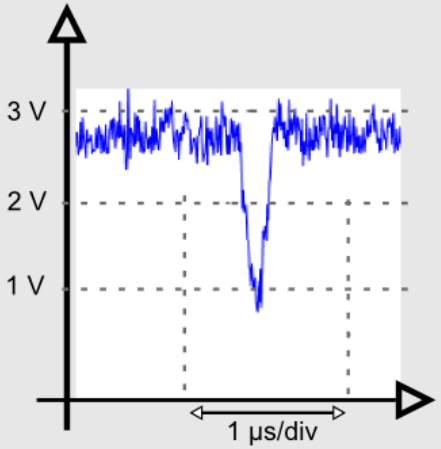
GIAnT: Hardware Overview

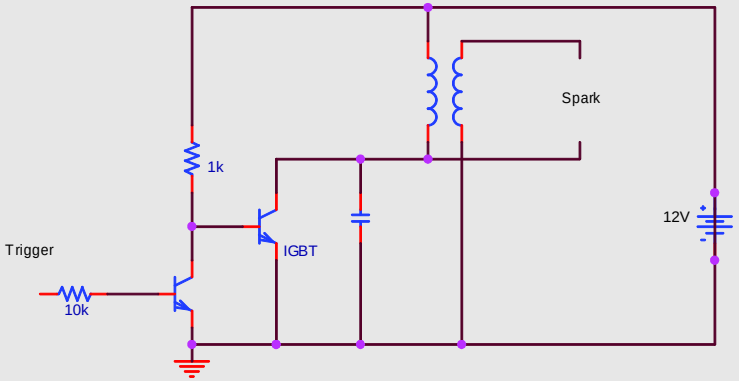


Fault Injection

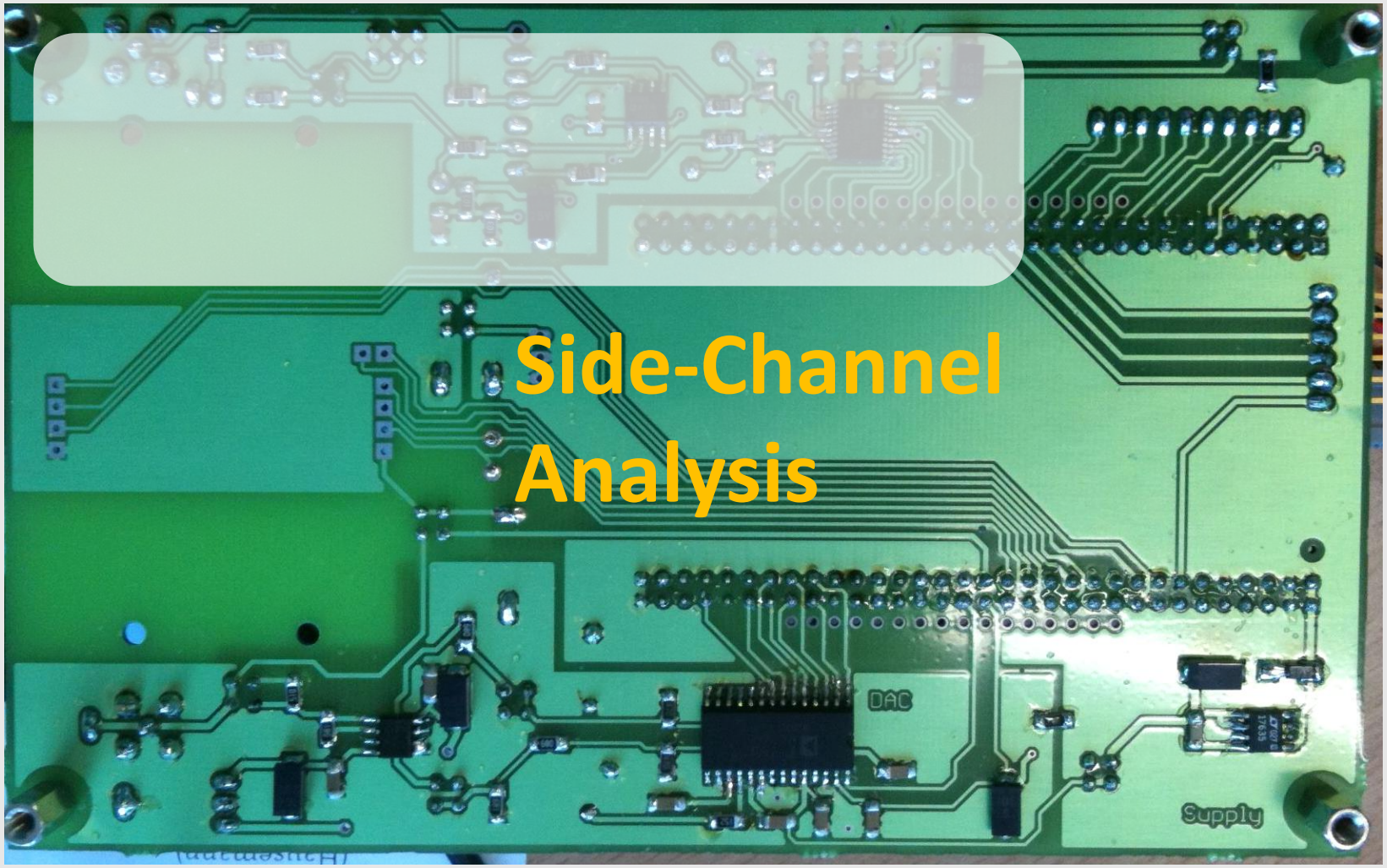
- Digital-Analog Converter AD9283
  - Up to 100 MHz (Resolution 10 ns)
  - Arbitrary waveform possible
  - Amplifier: -10 V … +10 V
- Extendable with external circuitry
  - Clock glitches
  - EM pulses
  - Laser







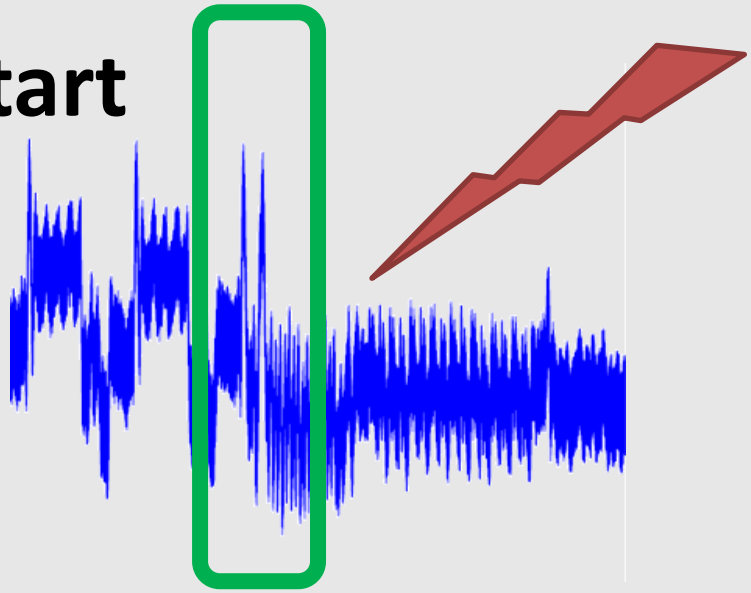
GIAnT: Hardware Overview



Side-Channel Analysis

- Analog-Digital Converter AD9283
  - Up to 100 MHz
  - 64 MB SRAM on FPGA module
- Record analog signals for side-channel analysis
- Pattern-detection for dynamic triggering

Detect start pattern



Dynamically inject fault

Fault injection

Practical Results

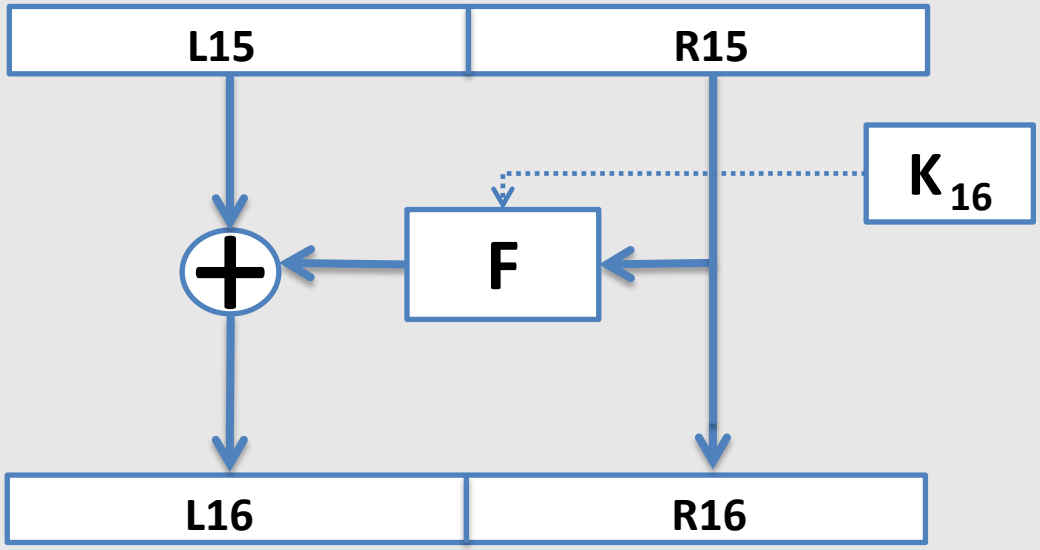
Practical Results: CRT-RSA on ATMega

- Atmel ATMega: Software CRT-RSA on „smartcard“

- Obtain faulty signature c' on x
- Lenstra: $d = gcd(x - (c')^e, n)$

Practical Results: 3DES on ATXMega

- Atmel ATXMega: Hardware DES engine
- Execute `DES` instruction 16 times
- Fault effect: Skip one round



- Recover K_{16}, iterate for full key

Let‘s hope the best and expect the worst

Live demonstration

Conclusion

GIAnT: Conclusion

- Fault injection and side-channel analysis
- **Low-cost**
- **Open source**
- Tested with various devices
- Continously being improved
  - RFID
  - Other fault injection methods
  - …
  - Contributions are welcome
- Visit sf.net/projects/giant

RUB

Thanks!
Questions?

hgi
Horst-Görtz Institut
für IT Sicherheit

David Oswald, Timo Kasper, Stephen Markhoff, Christof Paar
Chair for Embedded Security, Ruhr-University Bochum

EMSEC
EmbeddedSecurity