RUB

RUHR-UNIVERSITÄT BOCHUM

Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World

CHES 2011, Nara

September 30, 2011

David Oswald, Christof Paar

Chair for Embedded Security, Ruhr-University Bochum

hgi Horst-Görtz Institut für IT Sicherheit

EMSEC EmbeddedSecurity

Acknowledgements

- **Timo Kasper**
- **Christof Paar**

Outline of this talk

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

RUB

1. **Contactless Smartcards**
2. **Mifare DESFire** MF3ICD40
3. **DPA** on Mifare DESFire MF3ICD40
4. **Template Attacks** on Mifare DESFire MF3ICD40
5. **Lessons Learned**

A brief introduction

Contactless Smartcards

Contactless Smartcards: Overview

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

- **Contactless Smartcard** = RFID + Cryptography
  - **Secret key** on device
  - Cloning ≈ extract secret key
- Some applications
  - (Micro-)Payment
  - Passport
  - Public transport
  - Access control

Sources:
Wikipedia, cutviews.com

Contactless Smartcards: History

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

RUB

- First generation (around 2000):
  Mifare Classic, Legic Prime, TI DST, Hitag, ...
  - Proprietary cipher
  - Short key (max. 48 bit)
  - **Analytical attacks**
- **Today:**
  Mifare Plus, Legic Advant, Infineon SLE, SmartMX, Mifare DESFire (EV1), ...
  - Analytically secure
  - **Side-channel attacks**

Example

Mifare DESFire MF3ICD40

Mifare DESFire MF3ICD40 in a nutshell

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

- Introduced around 2002 by **Philips** (now **NXP**)
- **3DES** w/ 112-bit key for authentication and data encryption
- 4 kB non-volatile memory
  - 28 applications w/ max. 16 files each
  - 14 keys per application + 1 master key
  - Access rights on file level
- Based on asynchronous 8051 w/ 3DES engine
- “Glue logic”

Mifare DESFire MF3ICD40: Authentication protocol

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

RUB

Reader (PCD) | **DESFire MF3ICD40 (PICC)**

AUTH →

Generate 64-bit nonce n_c

$B_0 = 3DES_{k_c}(n_c)$

← **B0**

Choose B_1, B_2

B_1, B_2 →

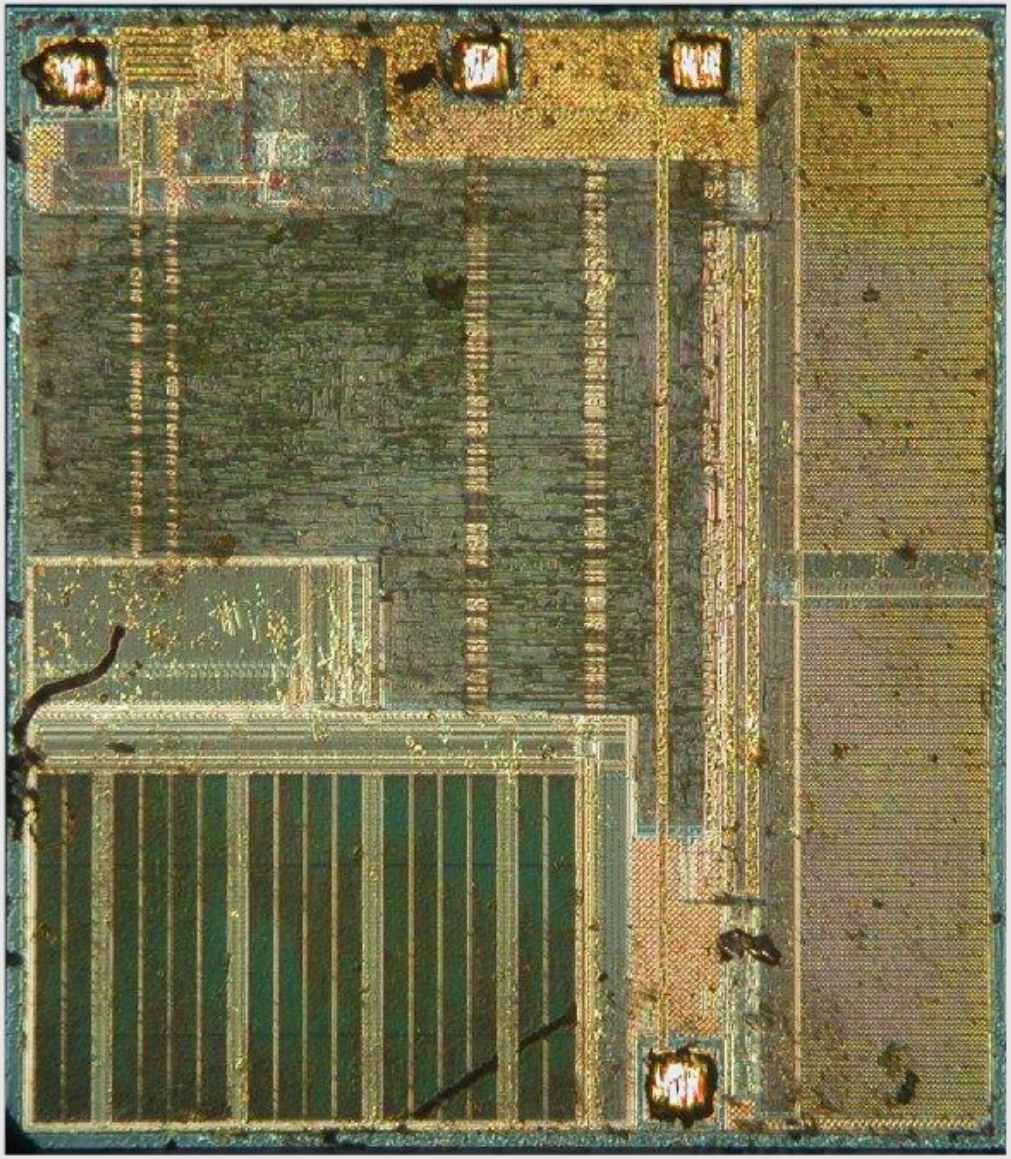
$C_2 = 3DES_{k_c}(B_2)$

$C_1 = 3DES_{k_c}(B_1)$

…

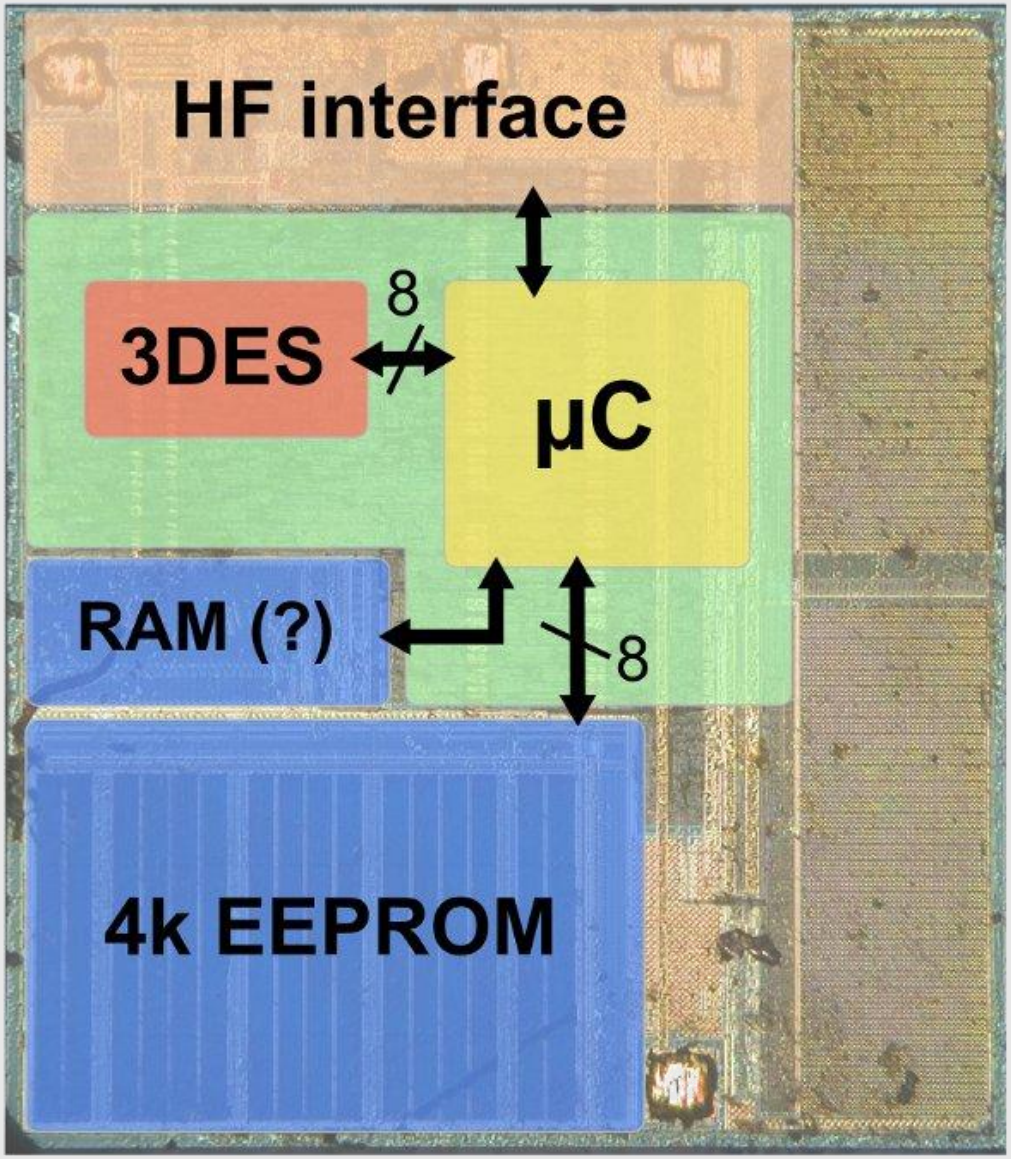
Mifare DESFire MF3ICD40: IC photograph

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar



Mifare DESFire MF3ICD40: IC photograph

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar



RUB

A walkthrough

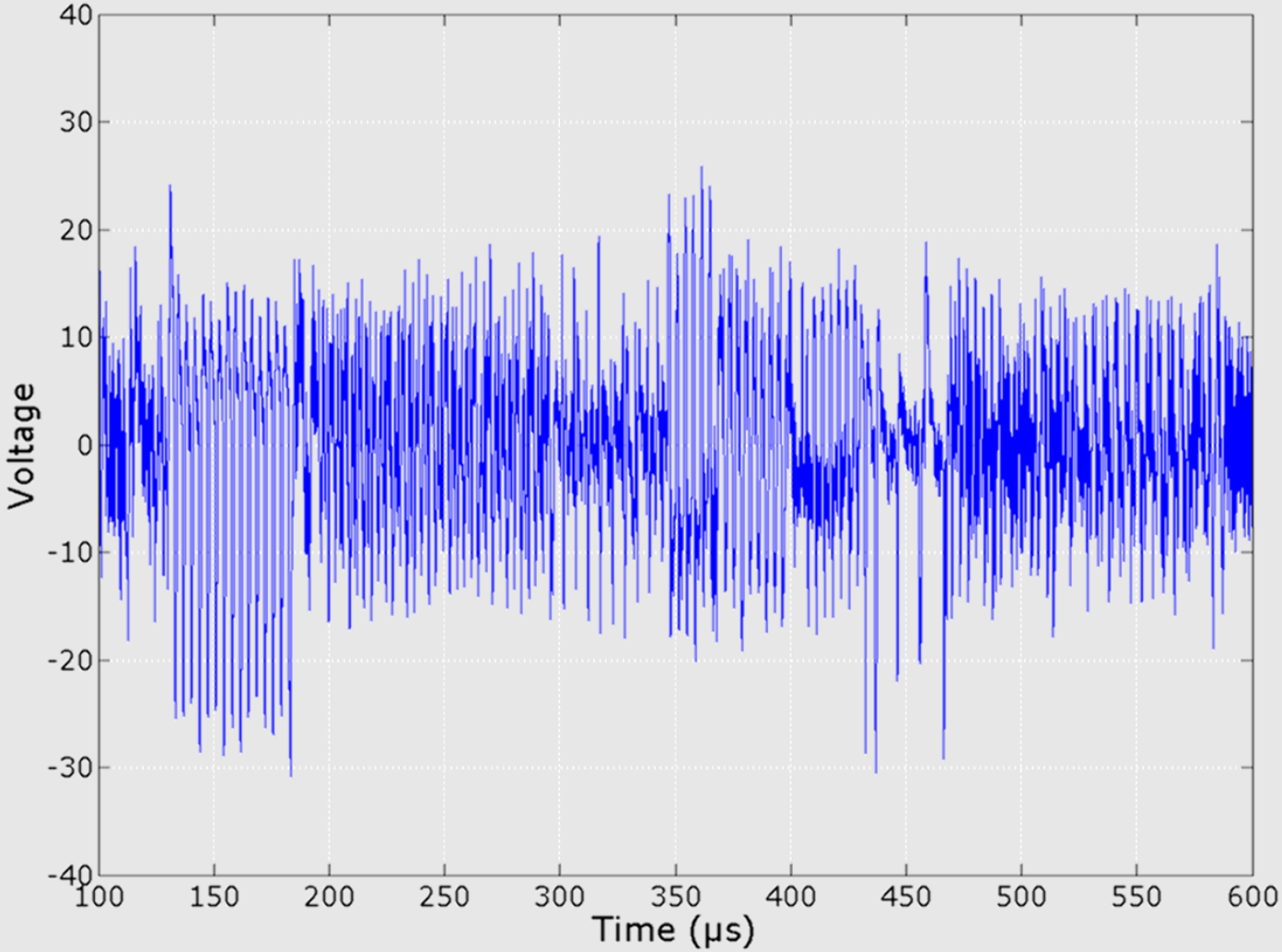
DPA on Mifare DESFire MF3ICD40

Mifare DESFire MF3ICD40: Preliminaries

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

RUB

Side-channel leakage of DESFire MF3ICD40 [RFIDSec11]

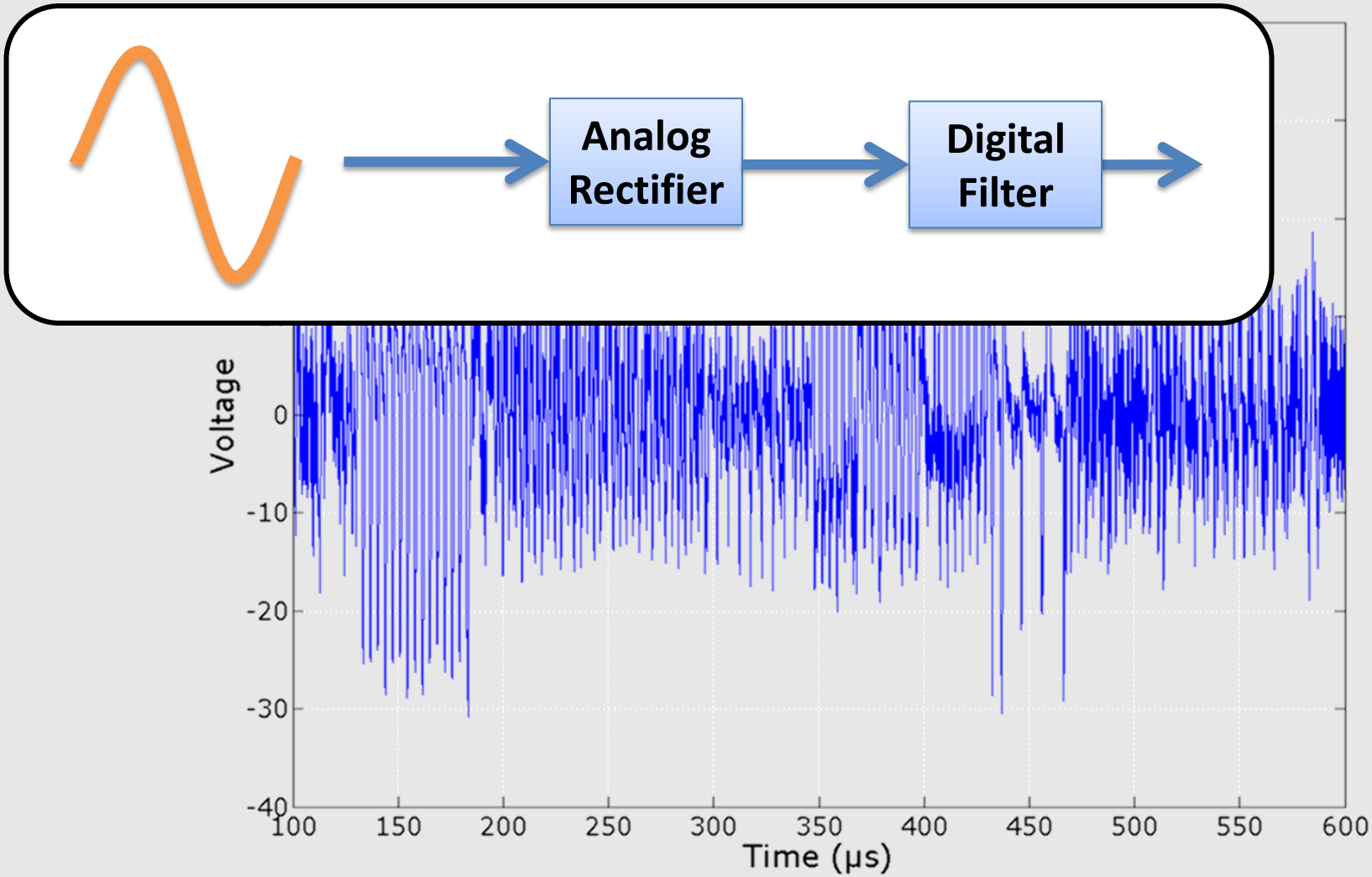


Mifare DESFire MF3ICD40: Preliminaries

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

RUB

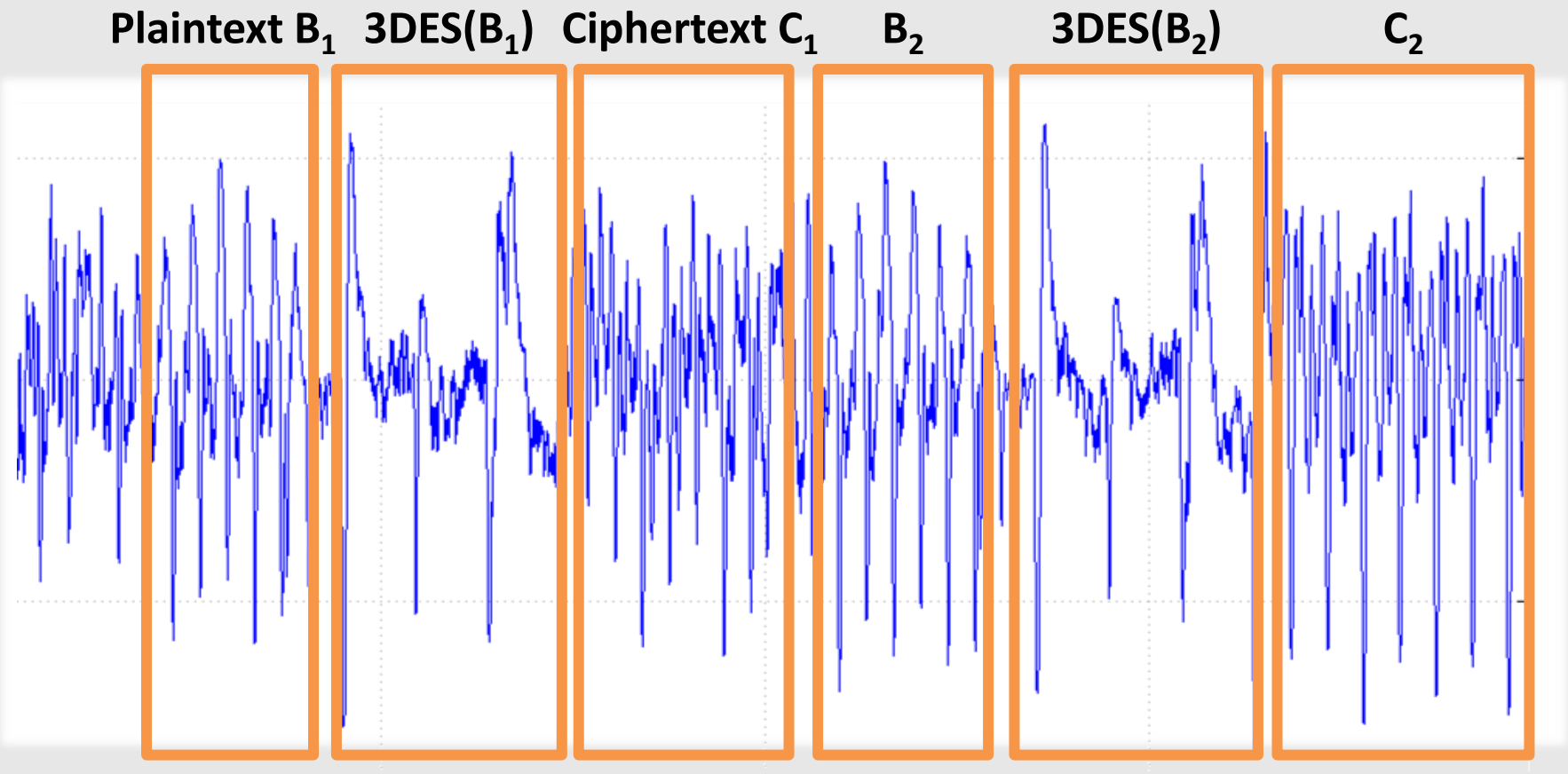
Side-channel leakage of DESFire MF3ICD40 [RFIDSec11]



Mifare DESFire MF3ICD40: Profiling

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

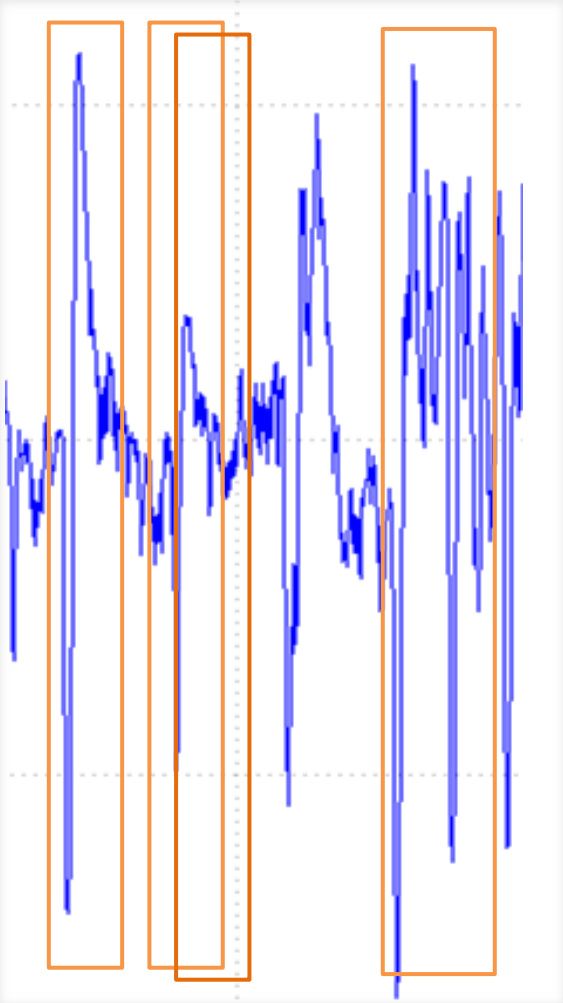
- **Step 1:** Understand device
- Locate plain-/ciphertext bytes using power analysis



DPA on Mifare DESFire MF3ICD40: Side-channel leakages

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

- **Operation:**
  $C = DES_{K1}(DES^{-1}_{K2}(DES_{K1}(B)))$
- Leakage 1: Bitwise **H**amming **D**istance of round 0→1 of $DES_{K1}(B)$, frequency domain
- Leakage 2: **H**amming **W**eight $DES_{K1}(B)$, time domain
- Leakage 3: **HD** round 0→1 of DES^{-1}_{K2}, freq. domain
- Leakage 4: **HW** of ciphertext C



DPA on Mifare DESFire MF3ICD40: Steps

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

RUB

Operation: $C = DES_{K1}(DES^{-1}_{K2}(DES_{K1}(B)))$

Goal: Recover *K1*, *K2* step-by-step

Perform DPAs on

1. **DES 1, round 1**: max. 48/56 bit of *K1* (250k traces)
2. **Full state after DES 1**: remaining bits of *K1* (150k traces)

---

3. **DES 2, round 2**: max. 48/56 bit of *K2* (250k traces)
4. **Ciphertext**: remaining bits of *K2* (< 2000 traces)

DPA on Mifare DESFire MF3ICD40: Management summary

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

RUB

- **Full key-recovery** with ~ 250k traces (~ 7 hours)
- **Low-cost equipment** ~ 2500 USD

⇒ High **threat potential**

- Opportunities for **optimization**
  - *Three* 3DES operations per trace, currently only *one* used
  - Improved signal processing (analog/digital)
  - Combine with *templates* (next part)

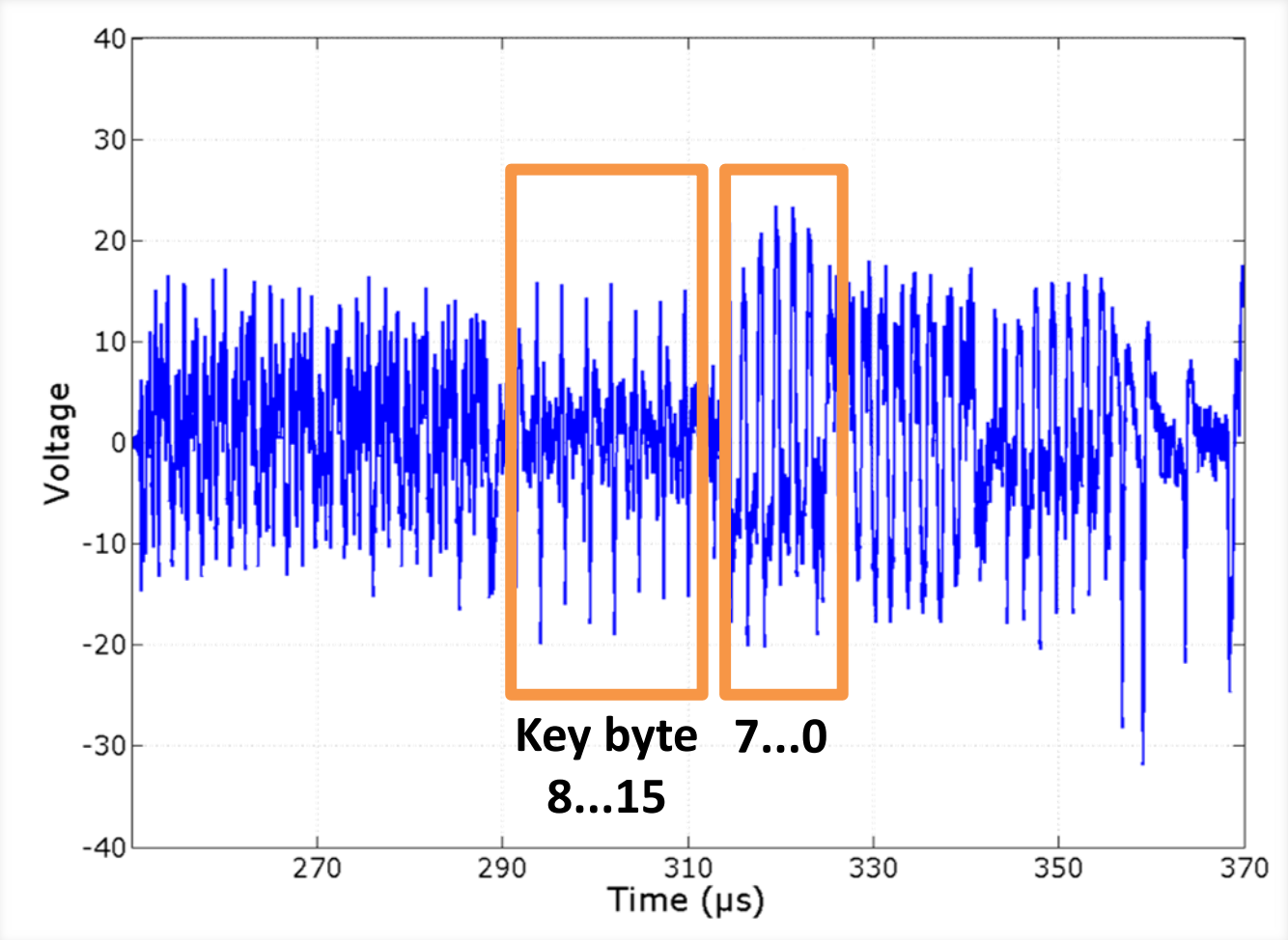
Other attack vectors

Template Attacks on Mifare DESFire MF3ICD40

Template Attacks on Mifare DESFire MF3ICD40: Idea

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

- 3DES I/O via 8-bit bus w/ **strong leakage**
- Including **byte-wise key transfer** ⇒ **template attack**



Template Attacks on Mifare DESFire MF3ICD40: Details

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

- 256 possible values per byte (ignoring parity)
- **Training set:** *1,024,000* traces ≙ *4,000* traces per value
- **Test set:** *1,024,000* traces
- Note: Byte 7... 0 ≠ Byte 8 ... 15
- Best results (average bit error rate)
  - 7 ... 0: **1.77 bit errors**
  - 8 ... 15: **0.51 bit errors**
- **Problem:** Leakage card 1 ≠ leakage card 2

Template Attacks on Mifare DESFire MF3ICD40: Management Summary

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

RUB

- Template attacks **in principle feasible**
- Possible improvements
  - More traces
  - Better classifiers

  } **Reduce error**

  - Calibration

  } **Card 1 → card 2**

- Currently: Limited threat
- **But:** Sometimes **profiling = matching device** (e.g. master key known before)

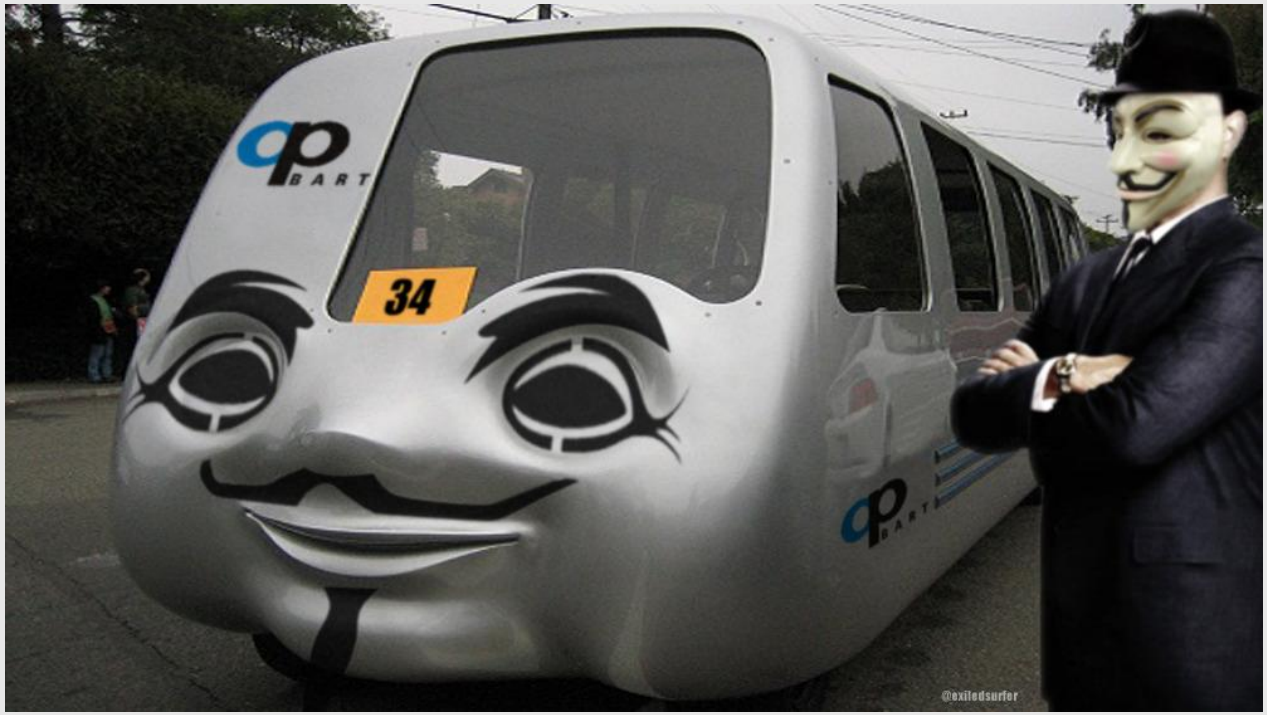
Conclusions and countermeasures

Lessons Learned

Lessons learned

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

- Power analysis = **Threat in real-world**
  KeeLoq 08, DESFire 11, Xilinx bitstream 11
- One-time engineering effort **high**
- **Then**: Attacks at low cost

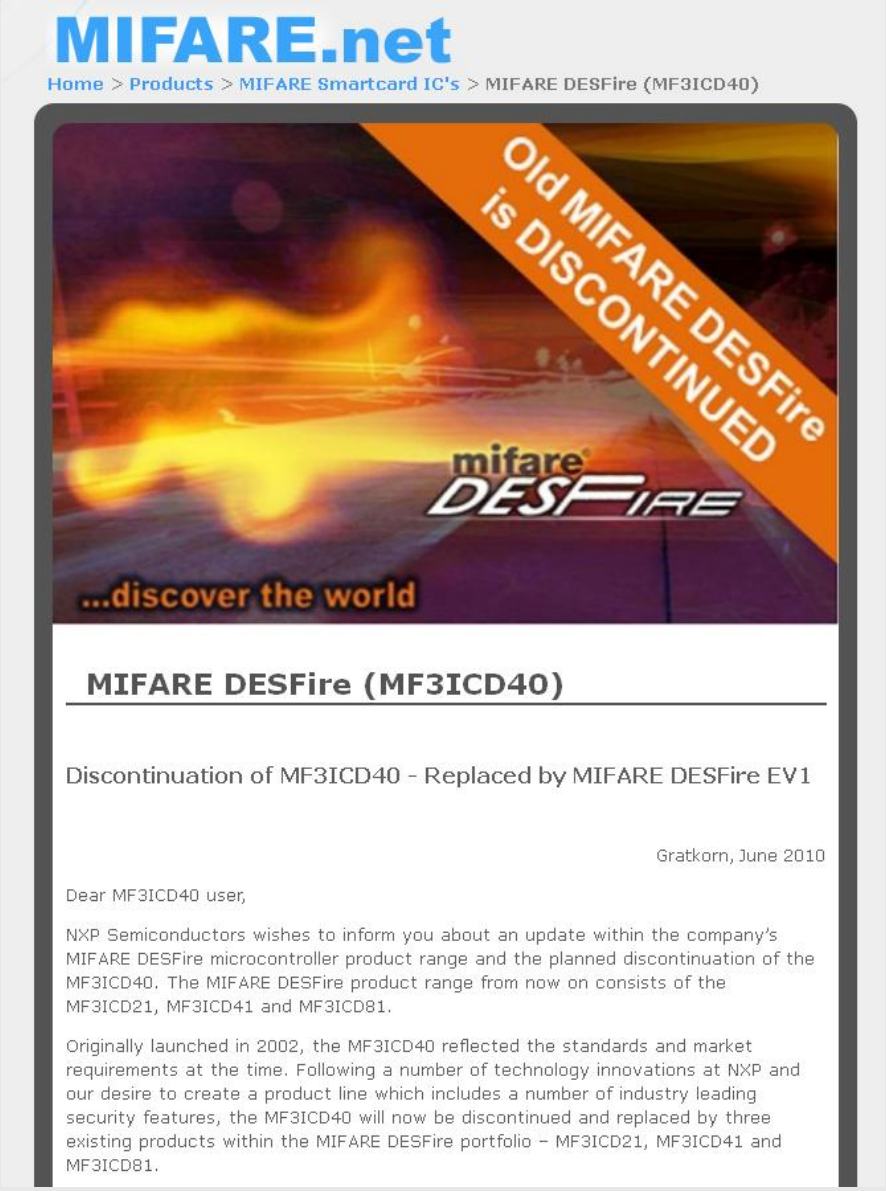


Source: @exiledsurfer

What to do?

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald
Christof Paar

- DESFire MF3ICD40 replaced by **DESFire EV1**
- Use **certified devices**
- Use **countermeasures** on the system level
  - Key diversification
  - Shadow accounts
- Follow ongoing **security research**



MIFARE.net

Home > Products > MIFARE Smartcard IC's > MIFARE DESFire (MF3ICD40)

Old MIFARE DESFire is DISCONTINUED

mifare DESFire

...discover the world

MIFARE DESFire (MF3ICD40)

Discontinuation of MF3ICD40 - Replaced by MIFARE DESFire EV1

Gratkorn, June 2010

Dear MF3ICD40 user,

NXP Semiconductors wishes to inform you about an update within the company's MIFARE DESFire microcontroller product range and the planned discontinuation of the MF3ICD40. The MIFARE DESFire product range from now on consists of the MF3ICD21, MF3ICD41 and MF3ICD81.

Originally launched in 2002, the MF3ICD40 reflected the standards and market requirements at the time. Following a number of technology innovations at NXP and our desire to create a product line which includes a number of industry leading security features, the MF3ICD40 will now be discontinued and replaced by three existing products within the MIFARE DESFire portfolio – MF3ICD21, MF3ICD41 and MF3ICD81.

Source: www.mifare.net

Thanks!
Questions?

David Oswald, Christof Paar
Chair for Embedded Security, Ruhr-University Bochum