"Henryk Ploetz and others have also posted documents on the internet containing detailed information which significantly facilitate attacks on cards and infrastructures using MIFARE Classic. NXP is trying to prevent these publications but due to the nature of internet it is to be expected that such an effort does not meet much success."

http://www.mifare.net/technology/security/mifare-classic/

Mikron

PHILIPS

SIEMENS

HITACHI

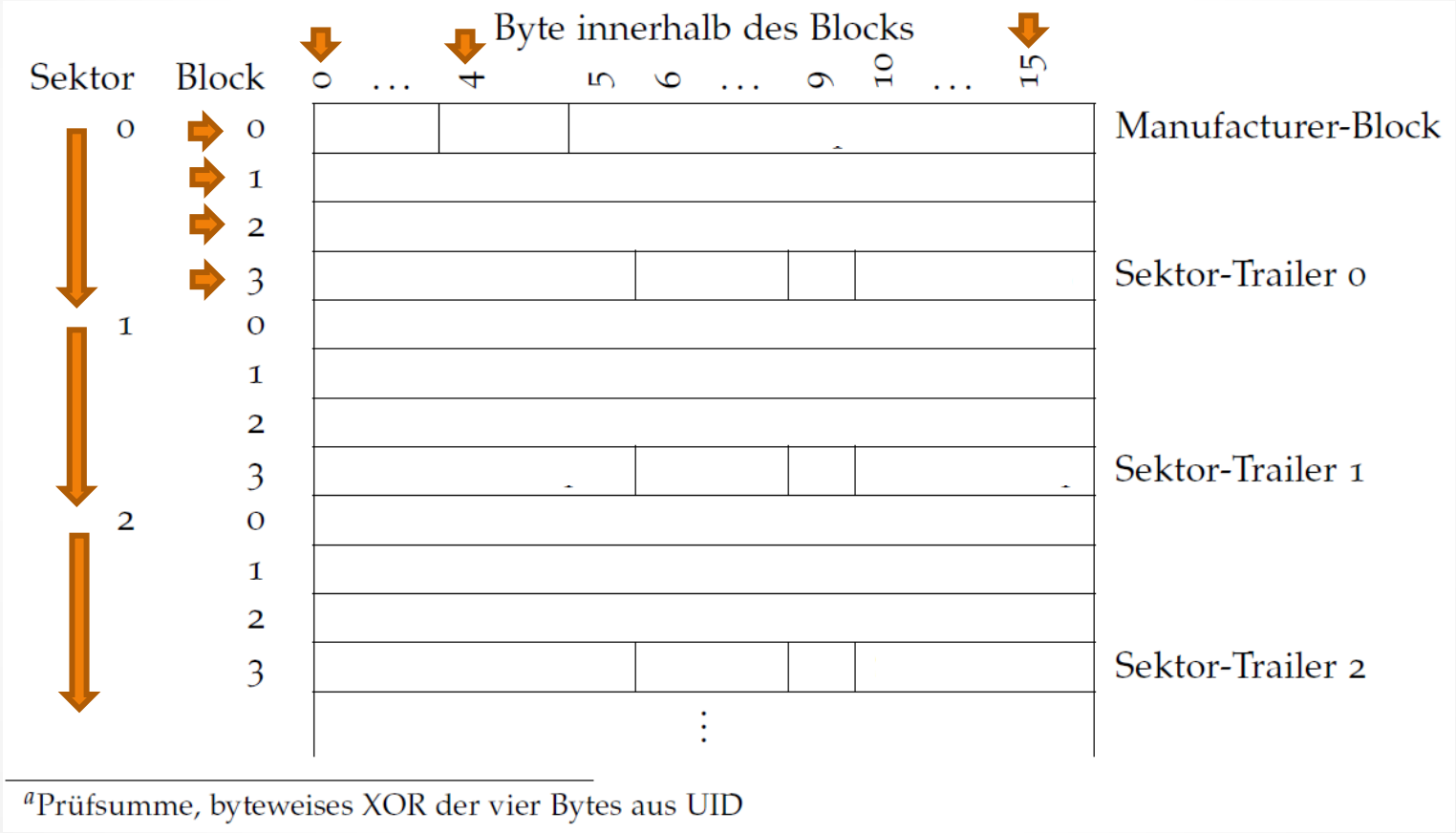
gemalto

security to be free

Portfolio

- MIFARE Classic
- MIFARE Ultralight
- MIFARE DESFire
- MIFARE Plus

MIFARE Classic Speicherlayout



- Henryk Plötz, Mifare Classic – Eine Analyse der Implementierung, S. 20 (2008)

MIFARE Classic ACL

ACLs legen fest

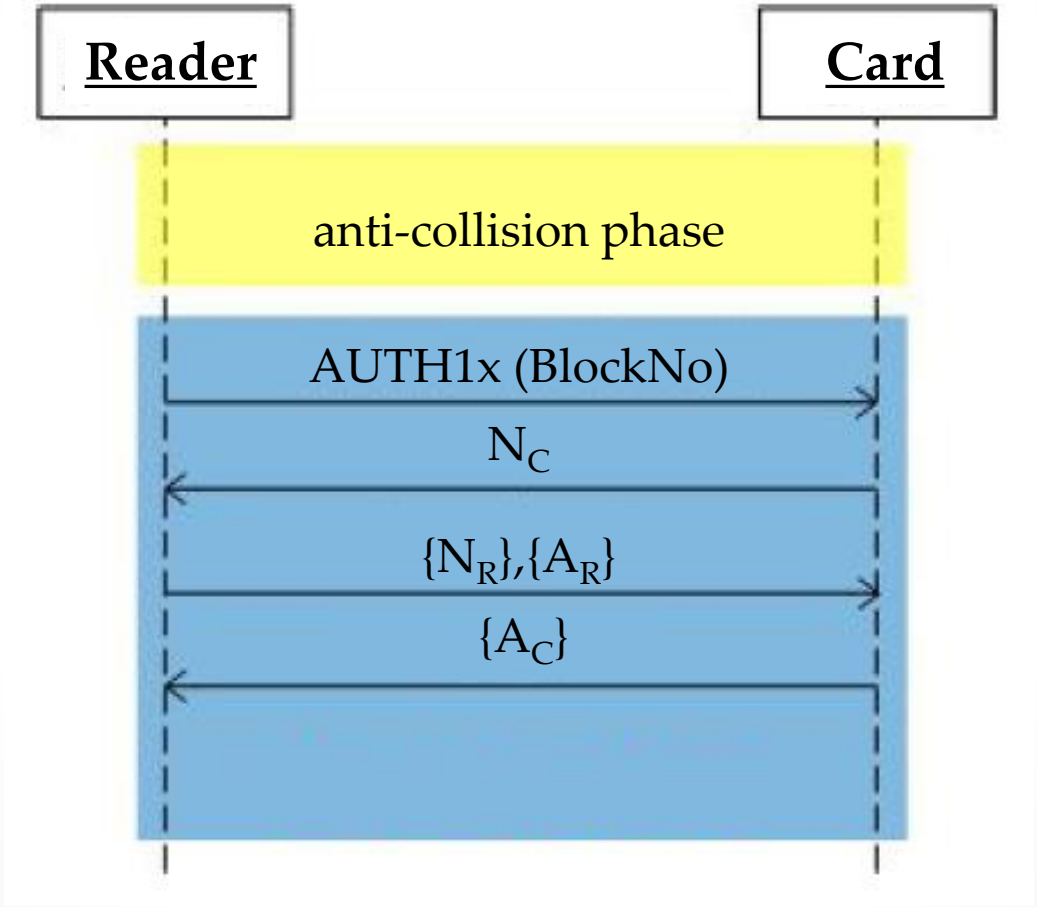
- read & write, read only, locked
- Block als Wertblock
  - Format: vorzeichenbehaftete 32 Bit Ganzzahl
  - Befehle: Inkrement, Dekrement, Transfer, Restore
- Unterschiedliche Rechte pro Key A und B

1 + 3: public Key A, reading / private Key B, writing

2 + 3: Fahrkatenentwerter enthält nur Key A mit Dekrement-Rechten

1+2+3: geschützte Kasse / Verkaufsautomat

MIFARE Classic Authentisierung

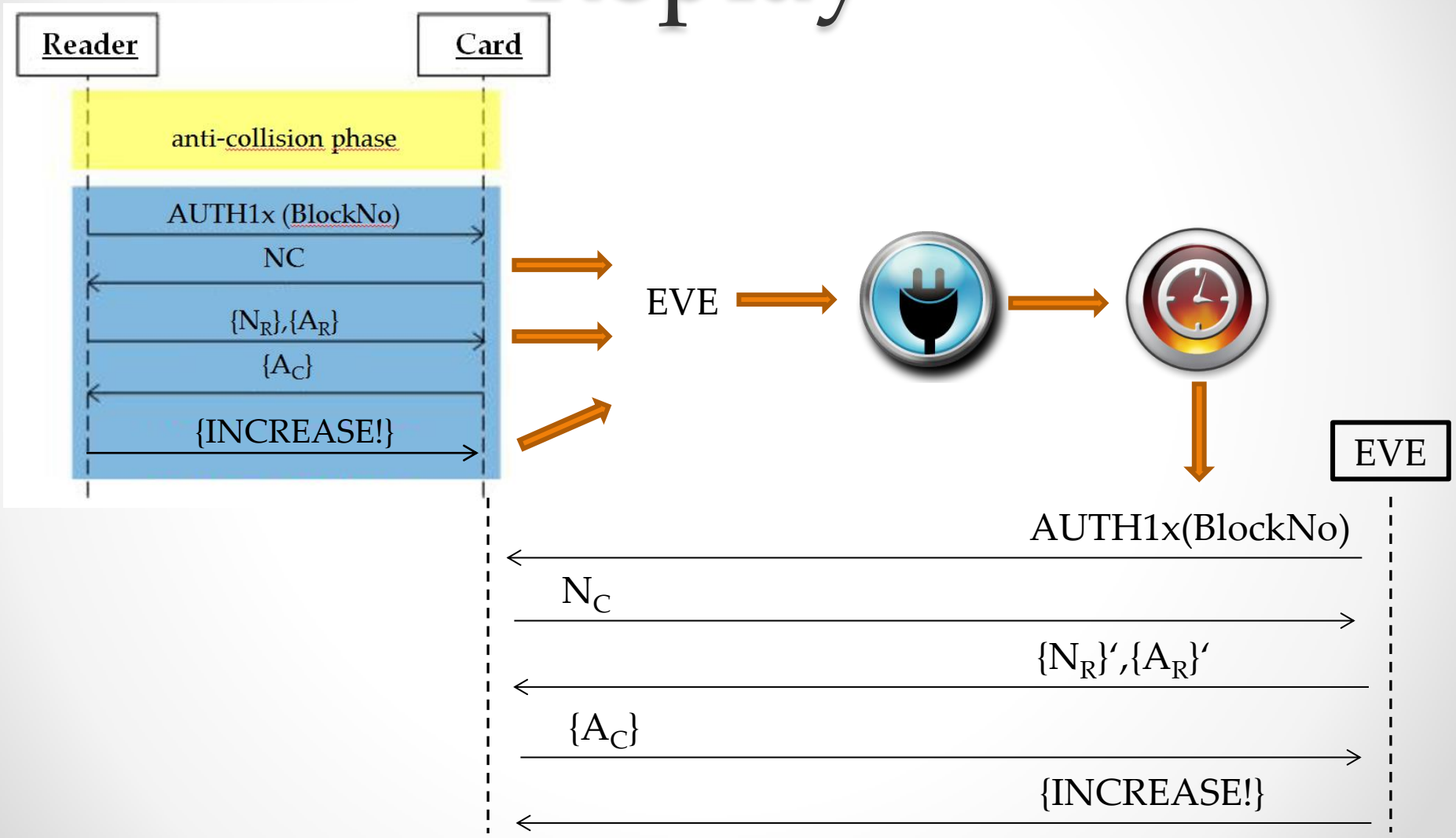


MIFARE Classic PRNG

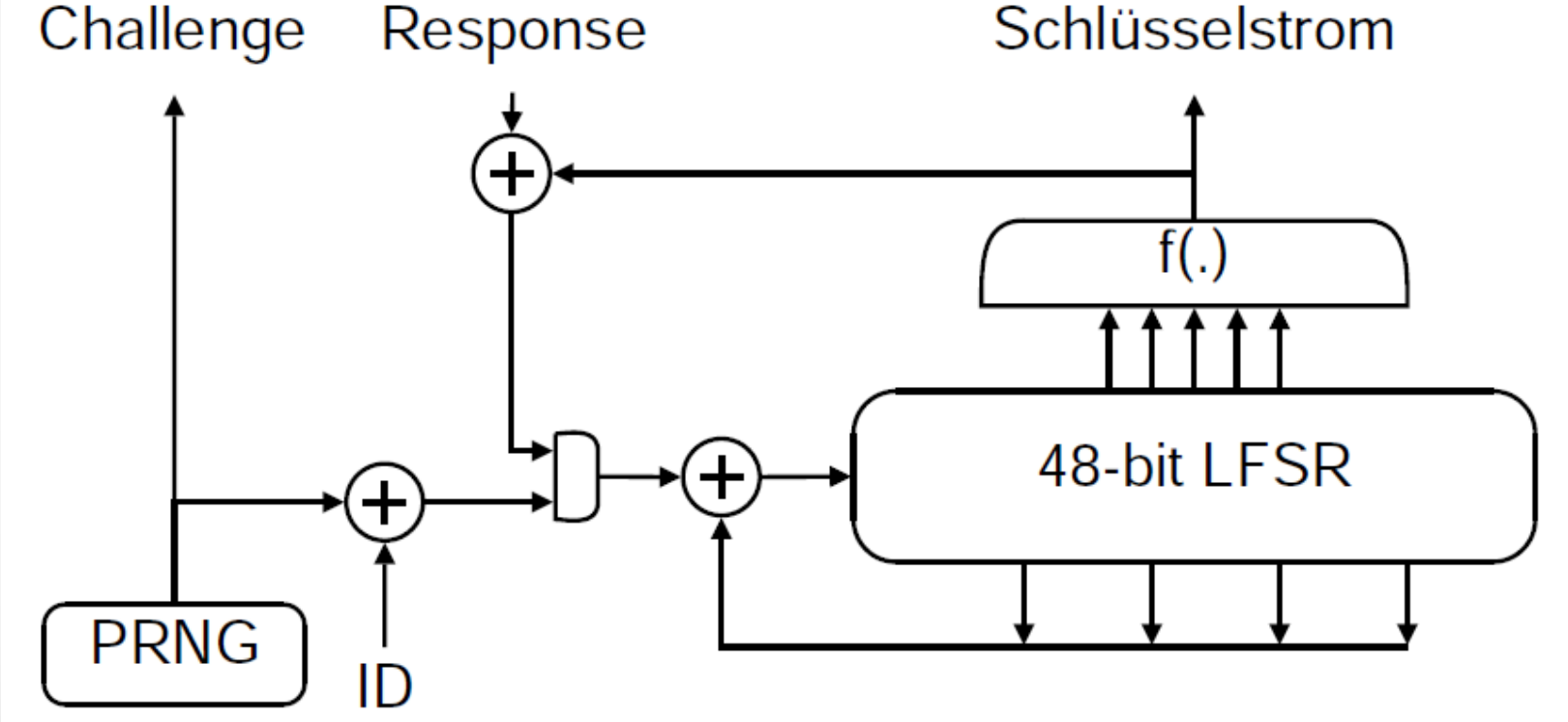
Pseudo Random Number Generator

- 16 Bit Registerbreite
- 2^{16} = 65.536 mögliche Nonces
- 0,62 s bis zur Wiederholung
- Fester Wert zur Initialisierung des Regsiters

MIFARE Classic Replay



MIFARE Classic Crypto1



MIFARE Classic Brute Force

48 Bit Key ~ 281,5 * 10^{12} Möglichkeiten

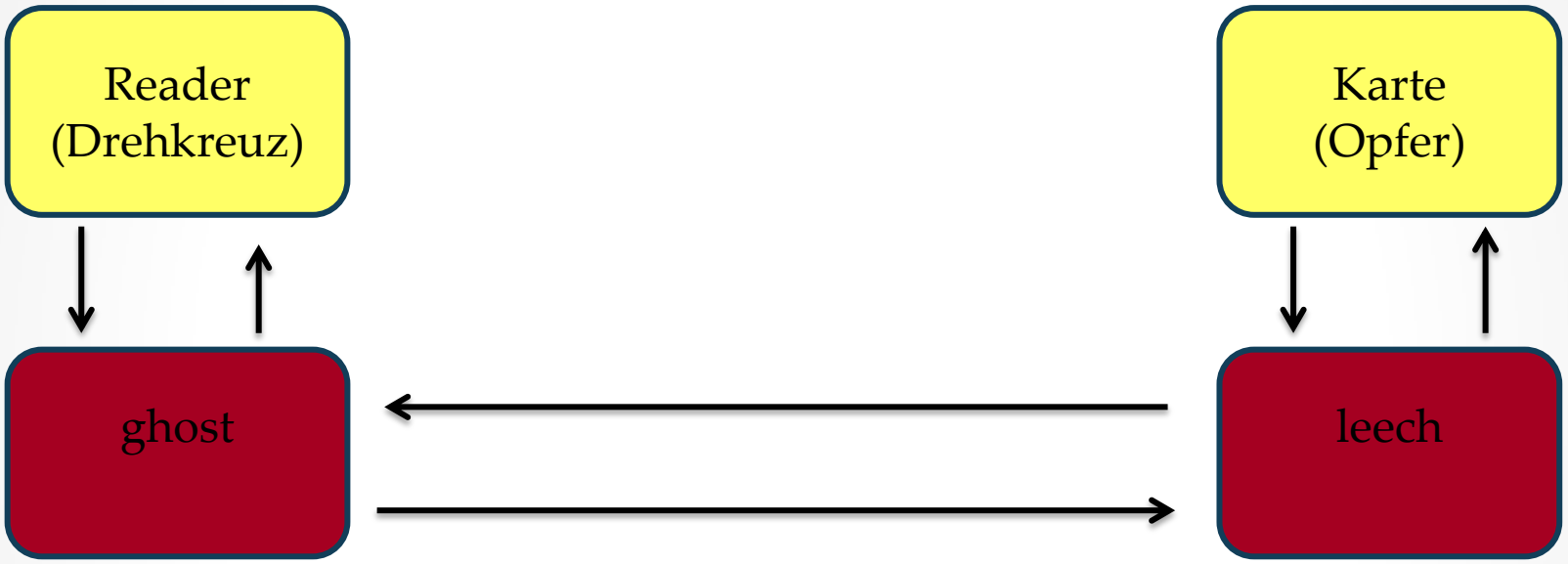
1. Versuchsaufbau

- 25 ms / Authentisierung
- 2^{48} Keys * 25 ms / Key = 222.985 Jahre
  -> 111.493 Jahre Erwartungswert

2. Leistung der Karte

- 6 ms / Authentisierung
  -> 26.758 Jahre Erwartungswert

MIFARE Classic Relay



MIFARE Classic Schwächen

- Geringe Entropie
- Nur jedes zweite Bit für den Keystream
- Ungenutzte Bits im Schieberegister
- Statistische Abhängigkeiten
- Wiederverwendung des One-time Pad
- Informationsabfluss durch Paritätsbits

=> Sehr schnelle Angriffe

MIFARE Classic Laziness

FFFFFFFFFFFF

A0A1A2A3A4A5

B0B1B2B3B4B5

4D3A99C351DD

1A982C7E459A

000000000000

D3F7D3F7D3F7

AABBCCDDEEFF

Quellen 1

NXP Zitat zu MIFARE Classic
http://www.mifare.net/technology/security/mifare-classic/

NXP MIFARE Portfolio
http://www.mifare.net/files/2513/0563/5124/NXP%20Z-card.pdf

Practical Attacks on the MIFARE Classic
by Wee Hon Tan (Imperial College London Department of Computing)
http://www.doc.ic.ac.uk/~mgv98/MIFARE_files/report.pdf
Practical-Attacks_MIFARE-Classic_mht.pdf

A Practical Attack on the MIFARE Classic
Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia
Radboud University Nijmegen
http://www.scriptworks.nl/gerhard/documents/mifare_weakness.pdf
mifare_weakness.pdf

Mifare Classic – Eine Analyse der Implementierung
Henryk Plötz
Humboldt-Universität zu Berlin
Oktober 2008
https://sar.informatik.hu-berlin.de/research/publications/SAR-PR-2008-21/SAR-PR-2008-21_.pdf

Quellen 2

Sicherheit Smartcard-basierter Zugangskontrollsysteme
Alexander Steffen
Ruhr-Universität Bochum
Januar 2012
https://www.emsec.rub.de/media/attachments/files/2012/04/Master-Arbeit-public.pdf

The MIFARE Hack
Mathias Morbitzer
Radboud University Nijmegen
http://www.proxmark.org/files/Documents/13.56%20MHz%20-%20MIFARE%20Classic/The_MIFARE_Hack.pdf

Cryptanalysis of Crypto-1
Karsten Nohl
University of Virginia
http://www.cs.virginia.edu/~kn5f/pdf/Mifare.Cryptanalysis.pdf

Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards
Nicolas T. Courtois, Karsten Nohl, and Sean O'Neil
https://eprint.iacr.org/2008/166.pdf

Quellen 3

4 Byte and 7 Byte ID usage for MIFARE Classic
http://www.mifare.net/files/4713/0936/9004/4-7_B_ID_Questions_Answeres_V12.pdf
4-7_B_ID_Questions_Answeres_V12.pdf

Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World – Extended Version
David Oswald and Christof Paar
Ruhr-Universität Bochum
http://www.emsec.rub.de/media/crypto/veroeffentlichungen/2011/10/10/desfire_2011_extended_1.pdf

Chameleon: A Versatile Emulator for Contactless Smartcards
Timo Kasper, Ingo von Maurich, David Oswald, Christof Paar
Ruhr-Universität Bochum
http://www.emsec.rub.de/media/crypto/veroeffentlichungen/2011/11/16/chameleon.pdf

Bildquellenverzeichnis

MIFARE Classic 1K Speicherlayout: Mifare Classic – Eine Analyse der Implementierung, S. 20
MIFARE Classic Crypto1: Mifare Classic – Eine Analyse der Implementierung, S. 53
MIFARE Classic Authentifizierung: Nach Vorlage von Practical Attacks on the MIFARE Classic, S. 26