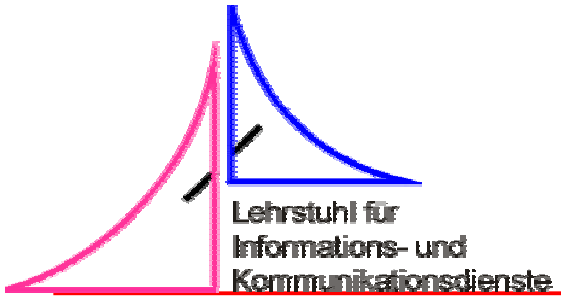
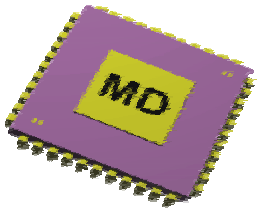
Workshop Bremen
Bedrohung aus Hardwaresicht

Prof. Clemens Cap
Dipl.-Ing. Igor Sedov
FB Informatik
Institut für Technische Informatik

Prof. Dirk Timmermann
Dipl.-Ing. Marc Haase
Dipl.-Ing. Hagen Ploog
FB Elektrotechnik u. Informationstechnik
Institut für Angewandte Mikroelektronik und Datentechnik





Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Gliederung

- Ursachen
- Klassifizierung von Angreifern
- Angriffsmöglichkeiten
- Möglichkeiten zum Schutz des Systems

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Ursachen

- Fehler bei der Implementierung von Algorithmen
  - Temporäre Speicherung von geheimen Daten
  - Plaintext wird nach Verschlüsselung nicht gelöscht
  - Speicherung von Schlüsseln auf unsicheren Medien (hotlists)
  - Key-recovery Datenbank

- Schwachstelle: Zufallszahlen-Generator
- Möglichkeit des Reverse Engineering bei mobilen Geräten, da in der Hand des Anwenders

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Klassifizierung von Angreifern (IBM)

Typen von Angreifern:

- Clever outsider
  - Intelligent, aber nicht ausreichende Kenntnis über das System
  - Ausnutzen von bereits bekannten Schwachstellen
- Knowledgeable insider
  - Technische Ausbildung und Erfahrung vorhanden
  - Unterschiedliche Kenntnis über Teilsysteme
  - Spezielle Software und Meßinstrumente vorhanden
- Funded organisations
  - Spezialisten-Team, großer Erfahrungsschatz
  - Detaillierte Untersuchung von Systemen
  - Entwicklung von speziellen Angriffsmöglichkeiten
  - Verwendung neuester Analysemittel

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Angriffsmöglichkeiten - Passiv

- Kryptoanalyse
  - known-plaintext attack
  - cypher-text attack
- Power-Analyse
  - Kenntnis über Architektur
- Angriff auf Protokoll-Ebene
  - Known-key attack
  - Replay

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Angriffsmöglichkeiten - Aktiv

- Versorgungsspannung
  - außerhalb des spezifizierten Bereiches
  - z.B. Analoger Zufallszahlen Generator generiert bei niedriger Spannung ausschließlich „1“
- Taktfrequenz
  - Single-Step-Angriff
- Temperatur
- Power & Clock Transients (Glitch)
  - Störung bei der Abarbeitung von Instruktionen in CPU

Folge:

- Fehlerhafte Instruktionen provozieren
- Auslesen des Speichers

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Angriffsmöglichkeiten - Physikalisch

- Entfernung des Chip-Gehäuses
  - Optische Untersuchung der Struktur
- Geräte
  - Laser Cutter Microscope
  - Hot Electron Analyzer
  - E-Beam Prober
  - Scanning Electron Microscope
  - micro-probing Meßsysteme
    - Zerstörung der Passivierung mittels Ultraschall
- Strahlung
  - Ionisierende Strahlung, UV-Licht
    - Veränderung von gespeicherten Daten

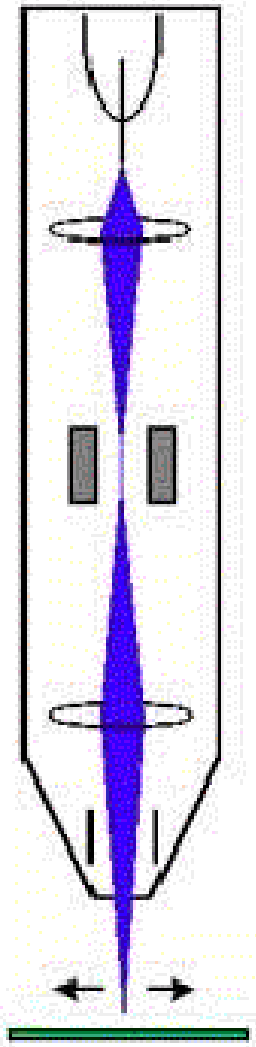
Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

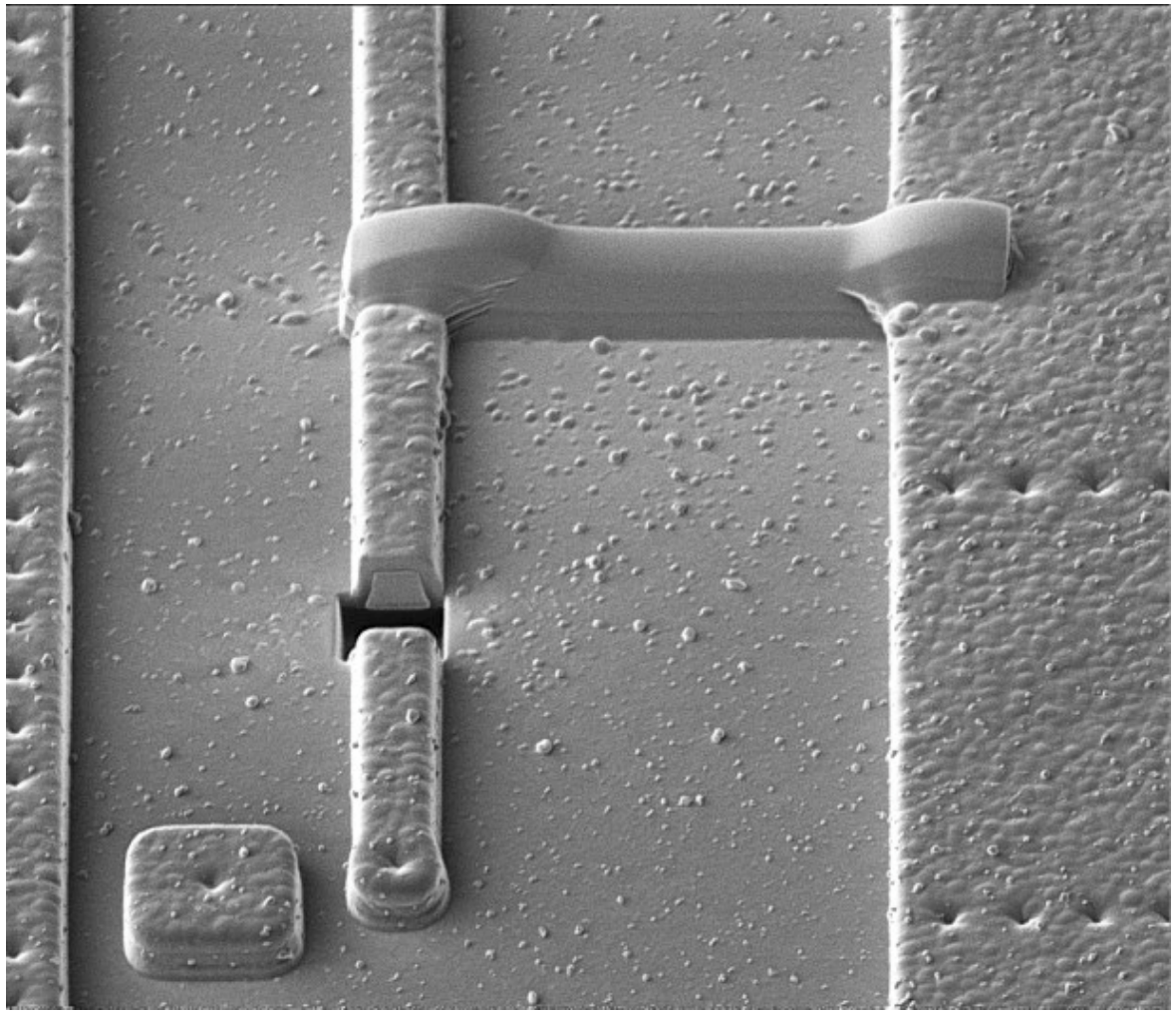
Angriffsmöglichkeiten - Physikalisch

- Layer Extrahierung (Intel 386)
- Beschichtung des Chips mit Metall (Schottky Effekt)
  - Erkennung von p&n dotierten Layern
- IBM: Beschichtung mit Lithium niobate
  - Analyse von Spannungsverhältnissen auf Chip
  - Auslesen mittels ultraviolettem Laser
  - 5V/25Mhz
- Durchleuchten von Silizium mittels Infrarot-Laser
- Focused Ion Beam (FIB)
  - Trennung von Verbindungen
  - Aufbringen neuer Verbindungen

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Focused Ion Beam - Beispiel





Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Veränderung von Speichern

ROM:

- Laser Cutter Microscope
- Veränderung von Bits
- Änderung im Programmcode (Sprünge)
- DES S-Box Modifikation => Verschlüsselungsfunktion linear

EEPROM:

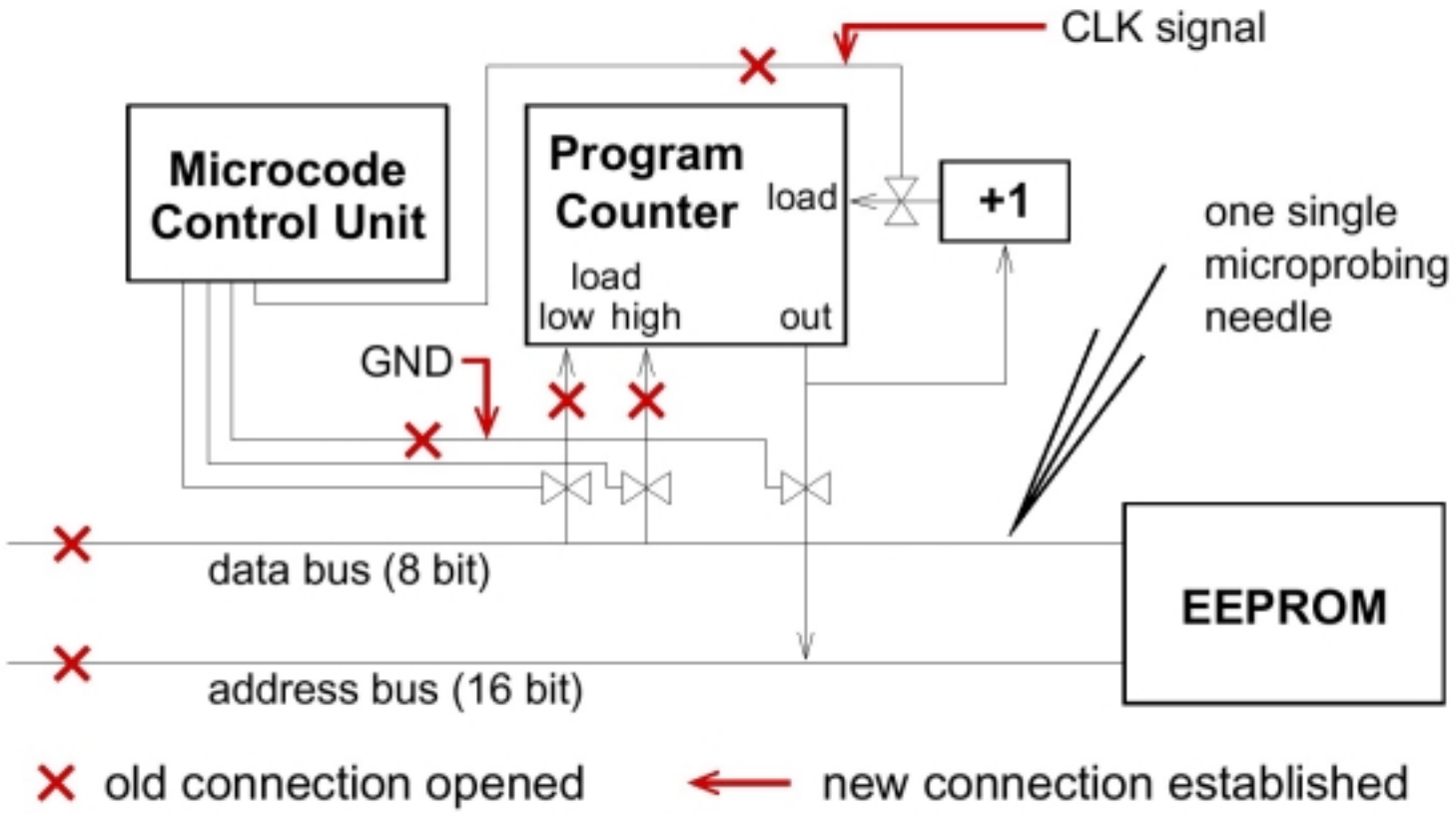
- Micro-Probe Nadeln zum Setzen oder Rücksetzen von Bits

RAM(stat./dyn)

- Ausnutzung des „Erinnerungsvermögens“

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Auslesen von geschütztem Speicher



Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Schutzmaßnahmen

- Sensoren:
  - Spannungs- und Taktüberwachung
  - Lichtsensoren
- Physikalischer Schutz:
  - Beständige Passivierung
  - Layout Veränderungen (obscure chip design)
- Verschleierung, Maskierung
  - Dummy Operationen
- Busverschlüsselung, Dummy Buszugriffe (Dallas-Chip)
- FIPS PUB Standard (IBM)

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Literatur

- Ross Anderson, Markus Kuhn, „Tamper Resistance – a Cautionary Note“
- Ross Anderson, Markus Kuhn, „Low Cost Attacks on Tamper Resistant Devices“
- Mehdi-Laurent Akkar et al., „Power Analysis, What is Now Possible ...“, Springer-Verlag Berlin Heidelberg 2000
- Counterpane Systems, „Security Pitfalls in Cryptography“, 1998
- Handbook of Applied Cryptography, A. Menezes, P. van Oorschot and S. Vanstone
- www.ibm.com

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de