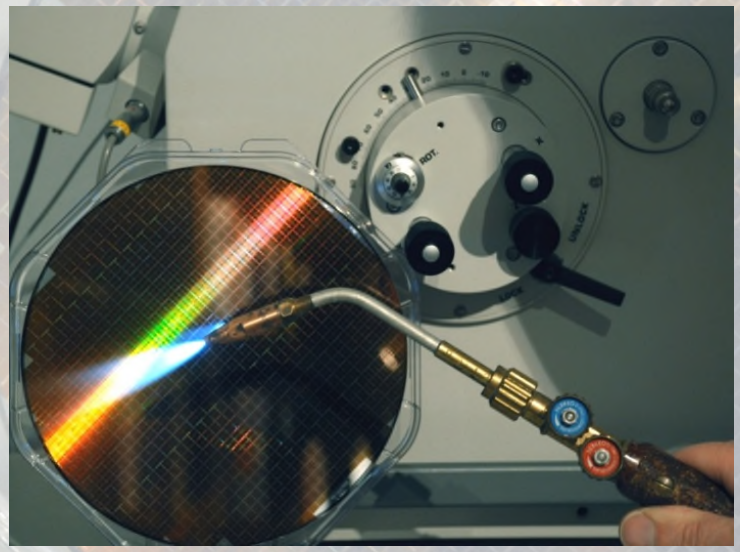
25 Jahre Chipkarten-Angriffe



Peter Laackmann
Marcus Janke

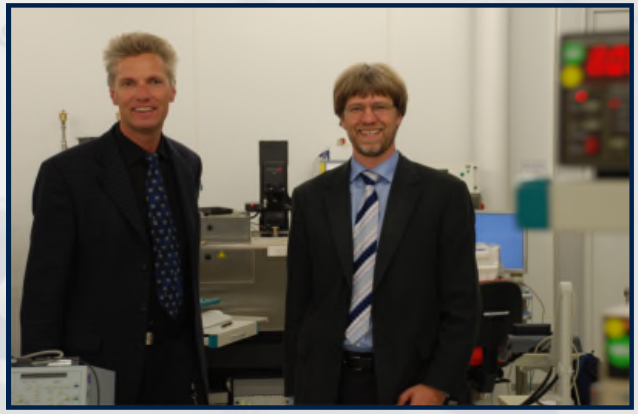
1989

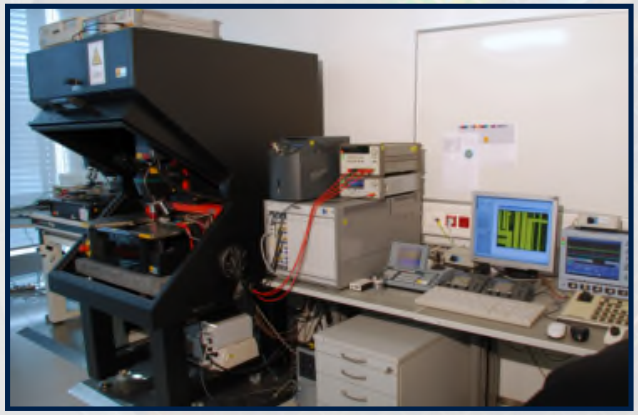
- Seit 1989: Chipkarten-Forscher
- Brunsbüttel, Kiel, Hamburg
- Reverse Engineering
- Fachautoren für Chipkartensicherheit
- Beratung Datensicherheit und Datenschutz
- Sicherheitsschwächen aufgedeckt:
  z.B. Krankenversichertenkarte, ec-Karte
- 1999 von Headhunter kontaktiert

Pictures: Private Archive M.Janke, P.Laackmann

2013

- Seit 1999: Mitarbeiter der Infineon Technologies AG
- München
- Chipsicherheit (Operativ&Strategisch)
- Leitung der internen Experten(“Hacker")gruppe
- Entwicklung neuer Angriffsmethoden
- Projektion teurer Angriffsmethoden auf Amateurmittel
- Private Forschung läuft weiter…



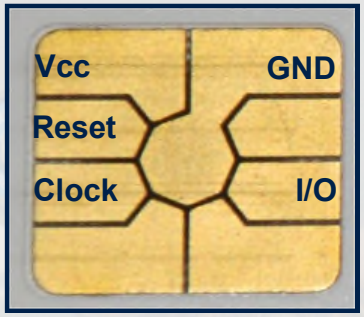


Pictures: M.Janke/P.Laackmann (Infineon)

Es War Einmal…Vor 25 Jahren

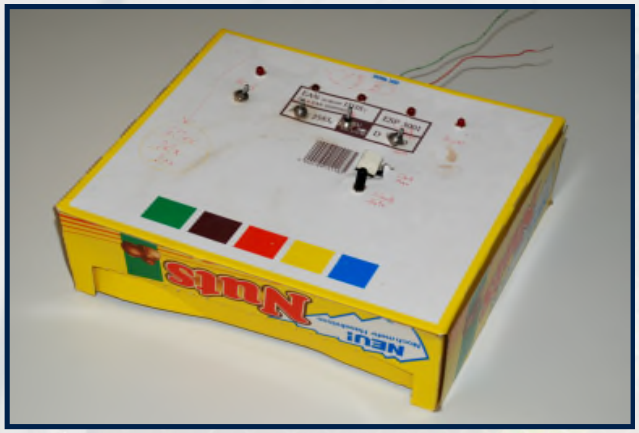
- Chipkarten waren NEU und kaum bekannt
- Die Technologie dahinter war nicht öffentlich
- Frage: Was verbirgt sich hinter den Gold-Kontakten?
- Reverse-Engineering war nötig! Jedoch...
- *Verbrauchte* Karten waren sehr selten
- *Neue* Karten waren teuer (12 DM oder 50 DM)
- Um Kosten zu sparen, zuerst nicht-destruktive Analyse

- Die Telefonkarten waren die ersten großflächig eingesetzten Chipkarten.
- Einfaches Design:
  - Speicher (EEPROM)
  - Kontroll-Logik
  - Keine CPU

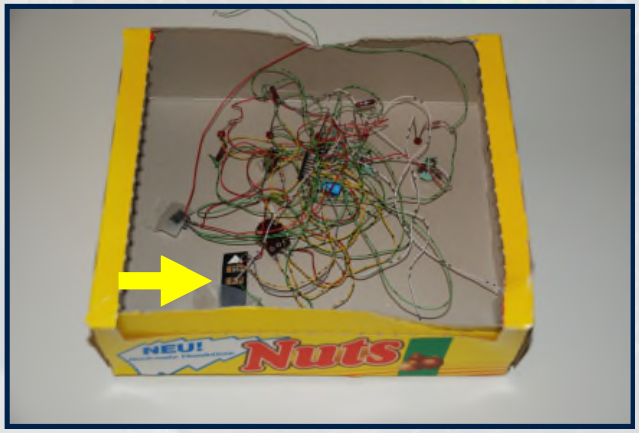


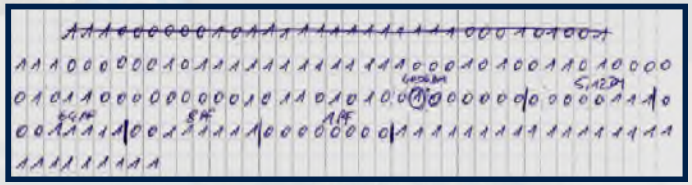
Pictures: Private Archive M.Janke, P.Laackmann

Es War Einmal…Vor 25 Jahren



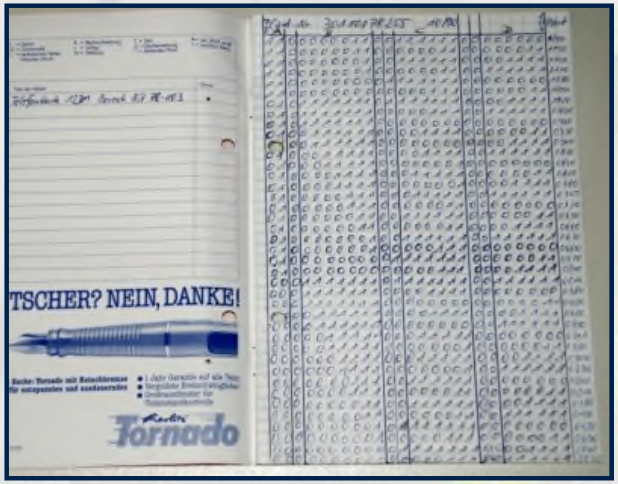
- Funktionale Analyse des Daten-Protokolls
- „Yellow Data Box“
- Enthielt ausgeschnittenen Telefonkarten-Chip (Pfeil)
- Clock&Reset werden mittels Taster bedient
- LED zeigt Datenausgang der Karte (I/O)
- Ausgabe wurde auf Papier mitgeschrieben





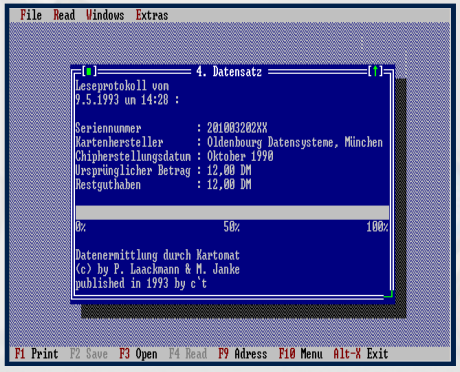
Pictures: Private Archive M.Janke, P.Laackmann

Es War Einmal…Vor 25 Jahren



- Schrittweises Abtelefonieren liefert Guthaben-Kodierung
- 12DM = 40 Einheiten = 40 Fahrten mit dem Fahrrad zur Telefonzelle…
- Danach Auswertung verschiedener Kartentypen

- Dann: Automatisches Lesen mit Commodore 64
- Kartenleser (Software und Hardware) für C64 (64‘er Magazin) und PC (C‘T) veröffentlicht



Pictures: Private Archive M.Janke, P.Laackmann

Chipkarten Heute - Anwendungen und Angriffsziele

Viele Anwendungen verwenden Chipkarten oder Sicherheits-Controller. Einige Beispiele:

- Bank- und Zahlungskarten
- Zugangskontrolle
- Identifikation, Pässe
- Öffentlicher Personen(nah)verkehr
- Mobiltelefone (GSM, UMTS)

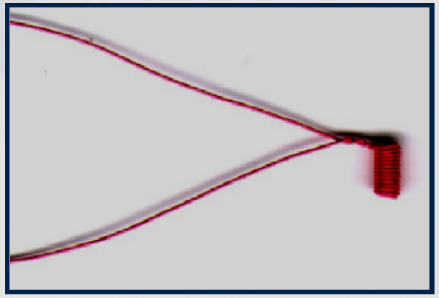
Angriffsziele sind hauptsächlich:

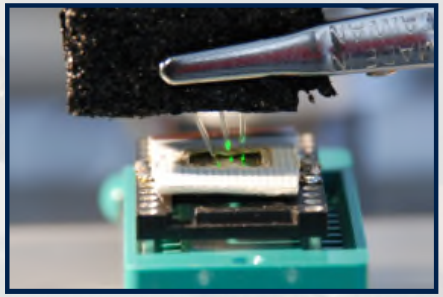
- **Ausspähen** geheimer Daten, um eine originale Karte zu duplizieren oder zu emulieren, z.B. Zugang oder ID → “Attack on confidentiality”
- **Modifikation** der Daten auf der originalen Karte, z.B. Geldbetrag, Zugangsrechte, Identität → “Attack on integrity”

Pictures: Private Archive M.Janke, P.Laackmann

Klassifizierung der Hardware-Angriffe

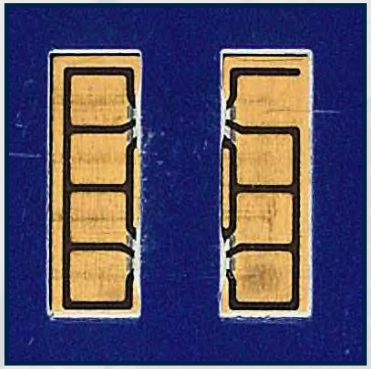
- **MANIPULATIVE Angriffe**
  - Probing, Forcing (Mikro-Nadeln, AFM, FIB)
  - Circuit Manipulation (FIB von Vorder- oder Rückseite, Lasercutter)
  - Zerstörendes Reverse Engineering (Ätzen, Schleifen der Chipstrukturen)
- **OBSERVATIVE Angriffe**
  - Timing Angriffe (TA)
  - Analyse des Stromverbrauchs (SPA, DPA)
  - Analyse der Elektromagnetischen Abstrahlung (SEMA, DEMA)
  - Optische Analyse (Optical Emission, SIL, OBIC, OBIRCH, LVP, Liquid Crystals)
  - Elektronenstrahl-Analyse (E-Beam, EBAC)
  - Reverse Engineering (z.B. Auslesen eines ROM, “Dekoration” durch Ätzen)
  - Verwendung von beabsichtigten oder unbeabsichtigten Backdoors
- **SEMI-INVASIVE Angriffe**
  - Indirekte Fehler-Induktion (Spikes, Glitches, Laser, Alphastrahlung, Röntgen, Elektronenstrahl, Hitze/TIVA, Elektrische Felder, Magnetische Felder, Elektromagnetische Induktion und viele mehr)
  - Direkte Fehler-Induktion (Signal-Einprägung mittels Mikro-Nadeln, AFM, FIB, On-top-Lithographie)





Pictures: Private Archive M.Janke, P.Laackmann

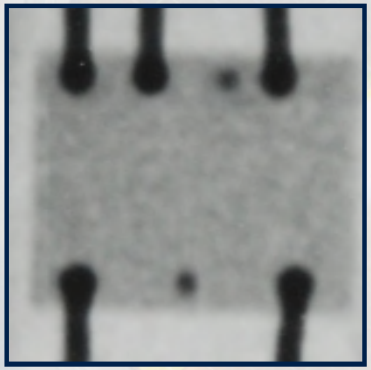
Manipulative Angriffe
HISTORISCHE Beispiele



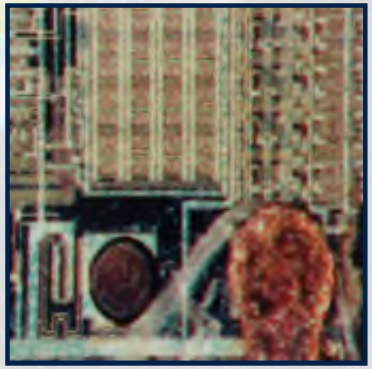
Chipmodul aus Telefonkarte,
Vergrößertes Kontaktfeld

“Fernseher”-Röntgenbild
zeigt Chip und Verbindungen

- Röntgenbild mittels eines alten Fernsehgeräts
- Röntgen-Streustrahlung belichtet Zahn-Film
- Mehrere Wochen Belichtungszeit
- Keine digitale Bildverarbeitung verfügbar, daher…
- Vergrößerung und Kontrasterhöhung im Photolabor
- 2 zusätzliche Pads entdeckt
- Pads mit Nadeln / Leitsilber kontaktiert



Vergrößertes Röntgenbild zeigt
2 zusätzliche Pads auf dem Chip



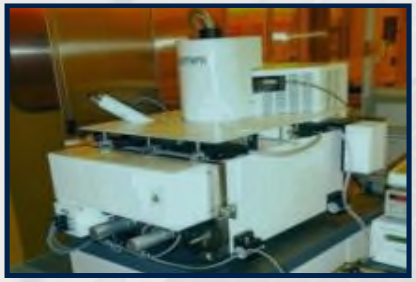
Eins der zusätzlichen Pads
nach Öffnung des Chipmoduls

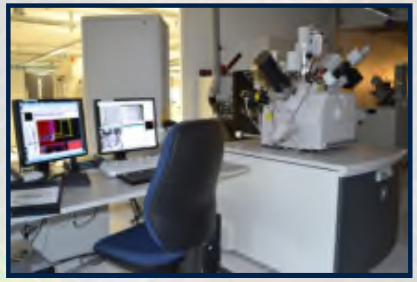
Originale Telefonkarte
in Vorderansicht

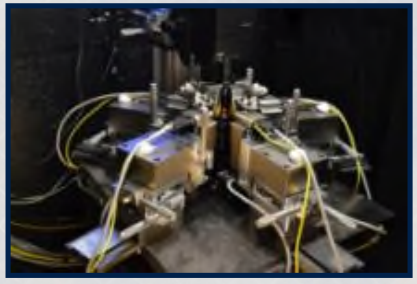
Die beiden zusätzlichen Pads
wurden nach extern kontaktiert

Pictures: Private Archive M.Janke, P.Laackmann

Manipulative Angriffe
PROFESSIONELLE Beispiele







Automatischer “Elektronenmikroskop-Chip-Scanner”
- Mikropositionierung des Chips mit Laser-Interferometer
- Positionierungs-Genauigkeit 50nm
- Erzeugt automatisch Bild-Mosaikteile mit Positionsdaten

Focused Ion Beam (FIB)
- Vorderseiten- oder Rückseiten-Angriffe
- Für praktisch alle modernen Chip-Technologien
- “Bohren”, Isolator ablagern, leitfähige Strukturen aufbringen
- Umgehung konventioneller Schutzstrukturen (Shields, Meshes)
- Bearbeitung von 22nm Chips mit 10 Metall-Lagen möglich

Atomic Force Mikroskop (AFM)
- Zeigt „n“ oder „p“ Dotierung im Chip, liest Speicherzellen aus
- Kann auch für Probing kleinster Strukturen verwendet werden

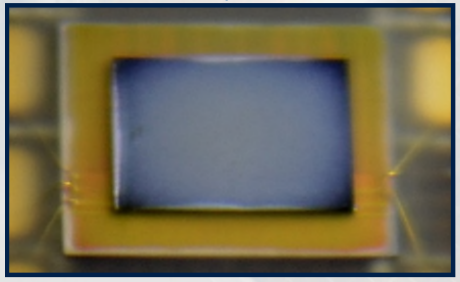
µProbe Station
- Direktes Kontaktieren von Signalen auf <65nm Chips
- Typisch 5 Nadeln gleichzeitig, lasergeführt
- Kontaktieren von einzelnen Zellen auf Chips

Pictures: M.Janke/P.Laackmann (Infineon)

Manipulative Angriffe
ZUKUNFTS-Ausblicke

Früher

Heute



Zukunft

IDEE: „CHIP gegen CHIP“

- Früher: Chip gegen Standard-Equipment (z.B. Oszilloskop)
- Heute: Chip gegen spezialisiertes Equipment (z.B. „DDK - Die Datenkrake“ [1])
- Zukunft: Chip gegen Chip (z.B. spezialisierter Angriffs-Chip, auf der Rückseite des “Victim” Chips aufgebracht)

[1] datenkrake.org

Realisierung: Lithographie auf der Chiprückseite

- Einfache Version: Neue Signalleitungen auf der Chiprückseite. Benötigt photoempfindliche Beschichtung, e-Beam oder Laser-Schreiber, Metallisierung und Ätzprozeß. Kontaktierung mit Rückseiten-FIB-Angriff.
- Verbesserte Version: FPGA auf der Rückseite des “Victim”-Chips. Benötigt besondere Verdrahtung auf der Angriffs-Chip Oberseite, um mit den herausgeführten “Victim”-Chip Signalen verbunden zu werden.
- High-end Version: Auf der “Victim”-Chip Rückseite wird ein eigener Chip erzeugt. Benötigt hochspezialisiertes Equipment.

Möglichkeiten: Multi-Probing und -Forcing in Echtzeit

- Probing und Forcing mehrerer Signale auf dem anzugreifenden Chip
- Echtzeitmöglichkeiten, Signalverstärkung und Signalanpassung
- Vorverarbeitung (Filterung, Komprimierung) der Signale

Pictures: Private Archive M.Janke, P.Laackmann (top, bottom) and D.Nedospasov (middle)

Manipulative Angriffe
AMATEUR Beispiele

Probing Station
- Gebrauchtes Equipment vom Online-Auktionshaus
- Auch ältere Geräte oft noch gut für Security-Chips

Selbsthergestellte Probing-Nadeln
- Wolframdraht (z.B. Trägerdraht aus Halogenlampen)
- Haushalts-Chemikalien: Natriumhydroxid (Rohrreiniger), Äthanol (Spiritus), Benzin, Tenside (Spülmittel)
- Chemisches Ätzen mit Prozess-Kontrolle liefert 200nm Nadelspitzen
- Microprocessor-kontrolliertes electrochemisches Ätzen liefert extrem feine (bis 5nm !) Nadelspitzen [1]

Atomic Force Microskop (AFM)
- Inzwischen als Kit für Schüler-Experimente erhältlich.

[1] O.L.Guise, J.W.Ahner, M-C.Jung, P.C.Goughnour, J.T.Yates, Reproducible Etching of Tungsten Probe Tips, Nano Letters 2002, 2(3), 191-193.

Pictures: Private Archive M.Janke, P.Laackmann

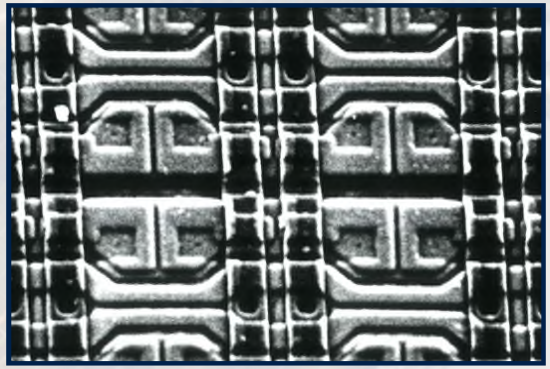
Observative Angriffe
HISTORISCHE Beispiele

Chip-Übersicht mit optischem Mikroskop

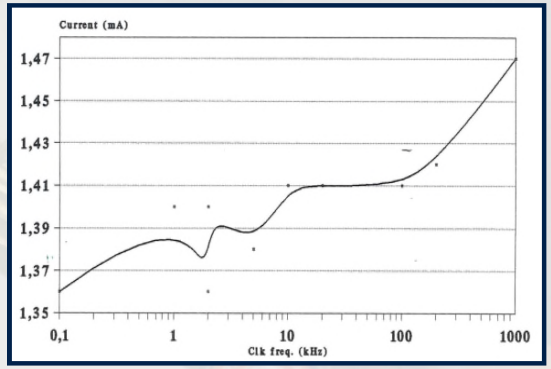
- Einfaches Mikroskop zeigte Chipstrukturen
- Zugang zu älterem Elektronenmikroskop
- Speicherstruktur und Funktionalitäten aufgedeckt

- Stromverbrauch über Frequenz gemessen
- Identifizierung einer zusätzlichen Sicherheitsfunktion

Älteres Elektronenmikroskop



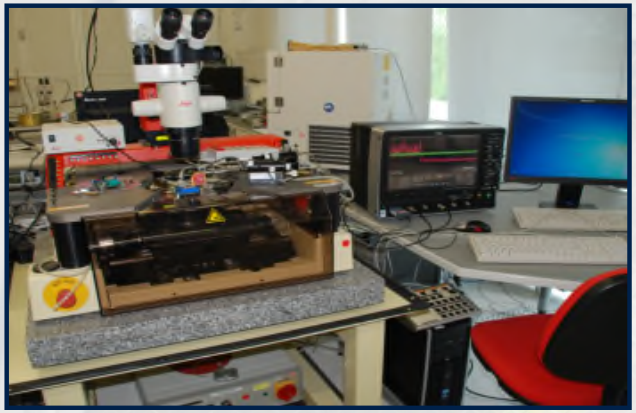
Speicherzellen im Elektronenmikroskop

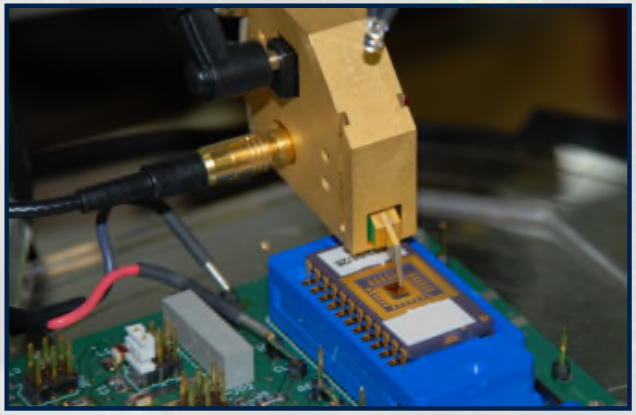


Stromverbrauchsmessung

Pictures: Private Archive M.Janke, P.Laackmann

Observative Angriffe
PROFESSIONELLE Beispiele





EMA/DEMA (Elektromagnetische Analyse)

- Auftragsgefertigte Mikrospulen-Sonde mit internem rauscharmen GaAs Verstärker
- Optionale Hoch-/Tief-/Bandpass-Filter
- Signal wird auf 40Gs/s Oszilloskop digitalisiert
- Speicherung der Digital-Meßwerte auf 2x 24TB RAID
- Preprocessing (vor der Schlüssel-Extraktion)
  - Digitales Filtern
  - Timing wird korrigiert (Jitter)
  - Viel Mathematik
- Danach mathematische Schlüssel-Extraktion.

Photonen-Emissions Analyse

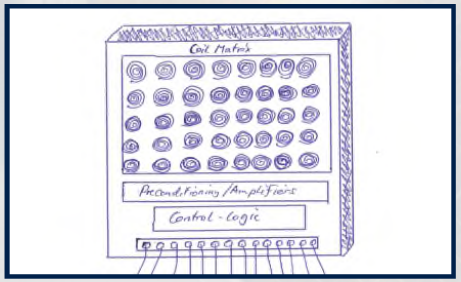
- Flüssigstickstoff-gekühlter IR-Detektor
- SIL (Solid Immersion Lens) Linsen auf Chiprückseite
- Infrarot-Laser zur gleichzeitigen Bestrahlung (OBIRCH)
- Navigation auf dem Chip mit IR-Transmission

Pictures: M.Janke/P.Laackmann (Infineon)

Observative Angriffe
ZUKUNFTS-Ausblicke

Früher

Heute



Zukunft

IDEE: „CHIP gegen CHIP“

- Früher: Chip gegen Standard-Equipment (z.B. DPA mittels Oszilloskop)
- Heute: Chip gegen spezialisiertes Equipment (z.B. „EMA Mikrosonden“)
- Zukunft: Chip gegen Chip (z.B. spezialisierter Angriffs-Chip mit EMA-Gitter, Kontakt-Visualisierung mit Infrarot, OLED Display-auf-Chip)

Realisierung: Angriffs-Mikrochips

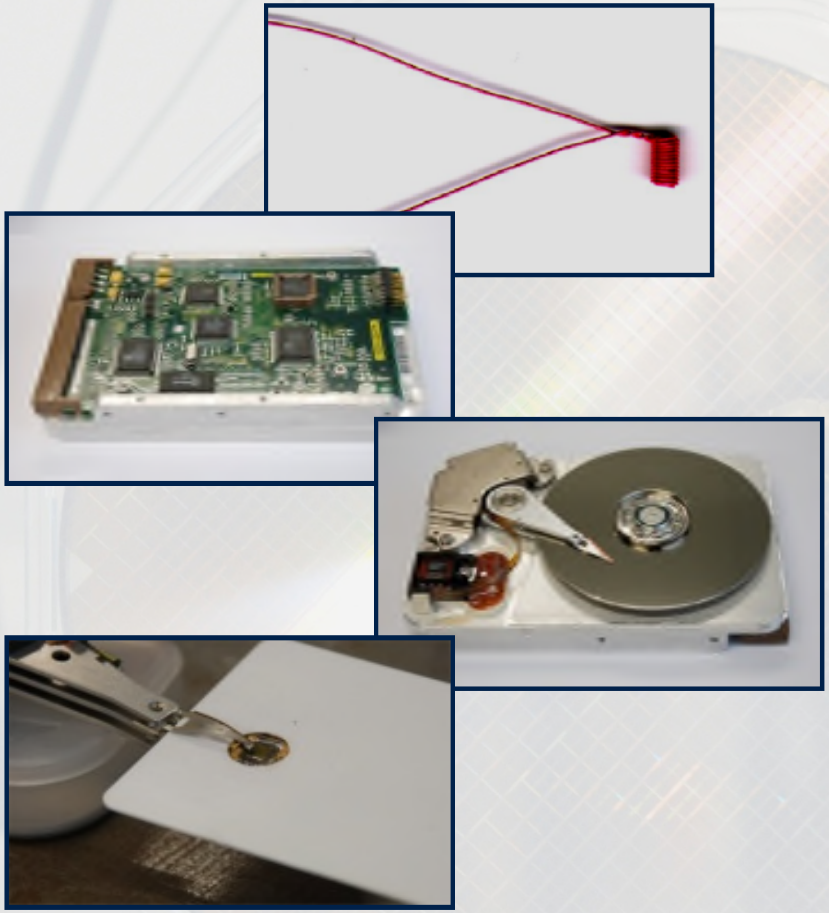
- EMA Grid-Chip: Spezialisierter Angriffs-Chip mit Mikrospulen-Array (Coil-on-chip). Coil-on-chip Technologien sind verfügbar, aber neues Chipdesign ist nötig.
- Kontakt-Imaging der Chiprückseite: Auf den “Victim” Chip wird direkt ein Imaging-Chip aufgesetzt, eventuell mit SIL (solid immersion lens) Methodik kombiniert. Benötigt spezialisiertes optisches Design und Chipdesign.
- OLED Display-on-chip: Signale werden auf der Chiprückseite mittels FIB-Rückseitenangriff herausgeführt und direkt auf dem Chip mit einer OLED Beschichtung visualisiert. Benötigt Beschichtungsprozess-Equipment und noch viel Forschung.

Möglichkeiten: Multi-Signal Beobachtung auf anzugreifendem Chip

- Beobachtung vieler Signale gleichzeitig auf einem Chip
- Signalverstärkung und Levelanpassung (EMA grid-chip)
- Signalaufbereitung und Vorverarbeitung (EMA grid-chip)

Pictures: Private Archive M.Janke, P.Laackmann

Observative Angriffe
AMATEUR Beispiele



- **EMA:** Billig-Sonden
  - Gewickelte Miniatur-Spulen aus Kupferdraht
  - Festplatten-Köpfe
  - Miniatur-Ferritspulen
- **EMA/DPA:** Digital-Oszilloskop und PC
  - Oszilloskop-PC-Einsteckkarte
  - USB Oszilloskop
  - Günstiges Digitaloszilloskop
  - Gebrauchtes Equipment
  - 1 bis 4 TB Festplatte für Meßwertspeicherung
  - DPA Freeware
  - Normaler PC
- **Photonen Emissions Analyse:** CCD IR Kamera
  - IR Kamera für Amateur-Astronomie
  - IR-Sensitiv
  - Peltier-gekühlte CCDs
  - Günstiges Infrarot-Mikroskopobjektiv (gebraucht)

Pictures: Private Archive M.Janke, P.Laackmann

Optical Fault Induction Angriffe
HISTORISCHE Beispiele

Sonnabend, 28. November 1981

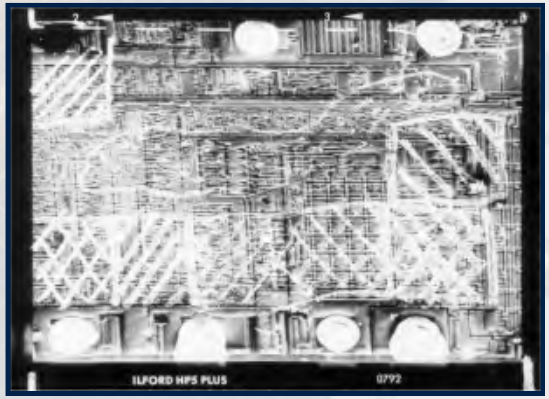
Laser macht es möglich

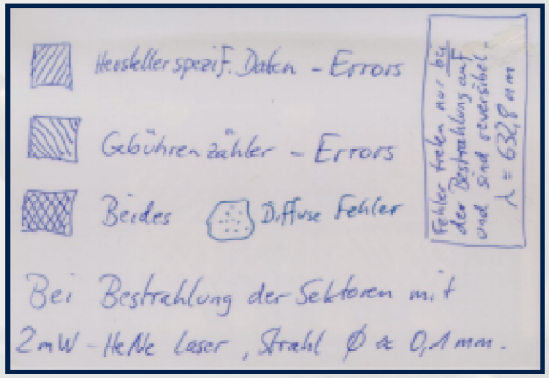
Kompletter Film auf einer Platte

Eine Laserröhre macht es möglich: Milliarden von Speicherpunkten auf einer Bildplatte, von einem haarfrei gebündelten Laserstrahl abgetastet, liefern einen kompletten Spielfilm. Die Bildplatte, die in einem Jahr auch in Europa auf den Markt kommt, wird auf einem Bildplattenspieler abgespielt. Der an jedes Fernsehgerät anzuschließen ist. Die sich 25mal in der Sekunde drehende Platte tastet ein Laserstrahl mit höchster Präzision von unten berührungslos und deshalb verschleißfrei ab. Dafür hat Siemens eine spezielle Laserröhre entwickelt (unser Bild). Farbbild und Stereoton sind auf der Platte als optische Punkte gespeichert.

Bei einer Umdrehung entsteht aus den Speicherpunkten einer haarfeinen Spur von nur 0,4 Tausendstel Millimeter Breite ein einzelnes Bild. Eine Stunde Spielfilm setzt sich aus 90 000 solcher Einzelbilder zusammen. Standbild, Zeitlupe und Zeitraffer vor- und rückwärts sowie ein gezielter Suchlauf zum schnellen Auffinden bestimmter Stellen sind besondere Möglichkeiten des Bildplattenspielers.

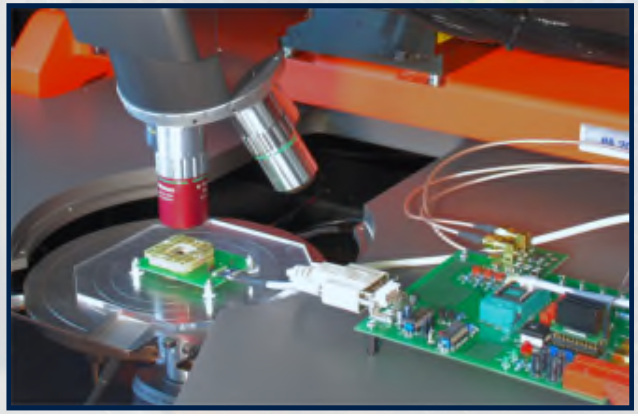
- 1992: Helium-Neon Laser aus VideoDisc Abspielgerät auf den Chip fokussiert, erzeugte selektive Fehler.
- Generelles Potential für Beeinflussung der Abläufe auf dem Chip wurde erkannt (“optical fault attacks”).





Pictures: Private Archive M.Janke, P.Laackmann

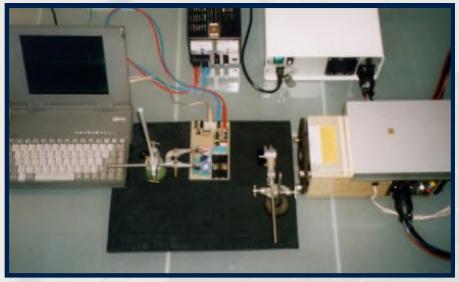
Optical Fault Induction Angriffe
PROFESSIONELLE Beispiele



- Automatisches Scannen des Chips (oder manuell)
- Chip sub-mikrometergenau in 3-Achsen positionierbar
- Dynamische Fokussierung über die Z-Achse beim Scan
- Verschiedene Wellenlängen in UV, VIS, IR
- Angriffe von der Vorderseite und Rückseite des Chips
- Navigation durch Infrarot-Durchstrahlung des Chips
- Multi-Spot (mehrere Laserstrahlen gleichzeitig)
    - Hauptsächlich genutzt gegen Software-Sicherheit sowie konventionelle Hardware-Sicherheitsfeatures.
- Multi-Shot (mehrere Laser-Schüsse, taktfein)
    - Hauptsächlich gegen Software-Sicherheitsfeatures
- Kombination mit anderen Angriffen (hybrid attacks)
    - Seeehr wirksam !

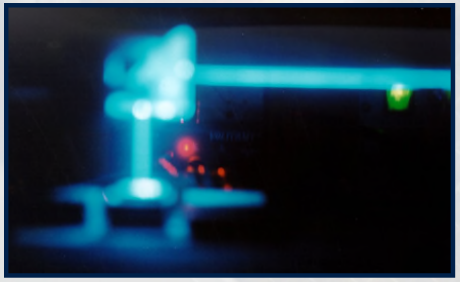
Pictures: M.Janke/P.Laackmann (Infineon)

Optical Fault Induction Angriffe
ZUKUNFTS-Visionen



Früher

Heute



Zukunft

IDEE: „CHIP gegen CHIP“

- Früher: Chip gegen Standard-Equipment (z.B. Laser auf Mikroskop)
- Heute: Chip gegen spezialisiertes Equipment (z.B. Multiple-Laser Angriff)
- Zukunft: Chip gegen Chip (z.B. DLP – Laser-Lichtsteuerung)

Realisierung: DLP (Digital Light Processing) / Spatial Modulators

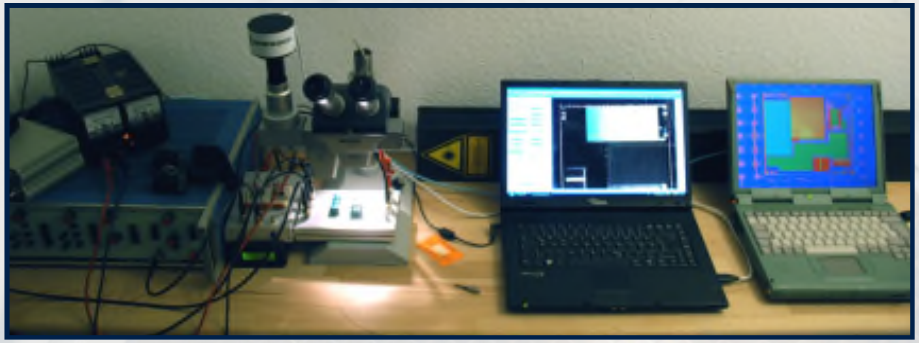
- DLP-Laser Kombination: Laserstrahl wird zeitlich und räumlich durch DLP-Spiegelarray gesteuert. Zusätzlich MHz-Modulation des Lasers. Benötigt besondere DLP Spiegelarrays, die der hohen Belastung durch die Laser-Energie standhalten.
- Räumliche Modulatoren: Holographische Lichtmodulation mit spezialisiertem Equipment. Benötigt aufwändiges optisches Design.
- Sehr große Parameter-Räume: Neue Konzepte benötigt.

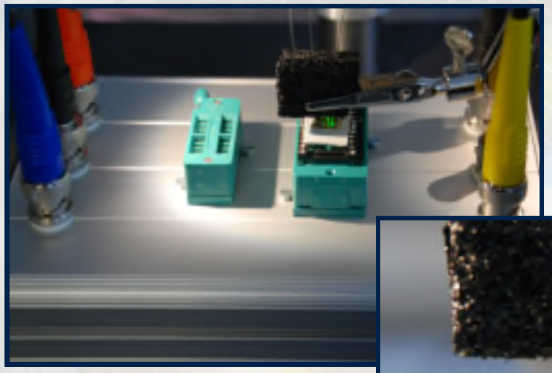
Möglichkeiten: “Multiple-area-multiple-time fault induction”

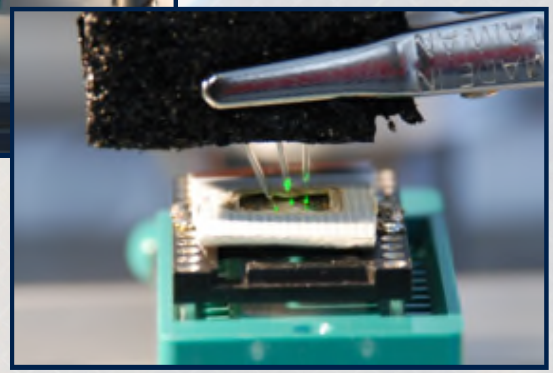
- Angriffsmöglichkeiten gegen eine Vielzahl von Software-Gegenmaßnahmen.
- Angriffsmöglichkeiten gegen viele Hardware-Gegenmaßnahmen.
- Schnelles “Mapping” von Sicherheitsfeatures auf einem unbekannten Chip.

Pictures: Private Archive M.Janke, P.Laackmann (top, bottom) and Infineon (middle)

Optical Fault Induction Angriffe
AMATEUR Beispiele







- Manuelles Positionieren (Mikrometerschrauben/Tische)
- Roter oder grüner Laser (e.g. DPSS laser, China)
- Infrarot-Laser für Angriff durch die Chip-Rückseite
- Laser in Kamera-Port des Mikroskops einkoppeln
- Laser mit Lichtleitfasern direkt auf Chipoberfläche leiten
- Multi-Spot Angriffe möglich
- Laser wird durch Software oder per FPGA getriggert
- 20kHz Modulation ist typisch für günstige (China) Laser

- Vorsicht: Starke Laser sind sehr gefährlich !
- Besondere Vorsicht bei Infrarot-Lasern !
- Risiko schwerster Augenschäden (und zwar für immer) !
- Nachlässigkeit lohnt sich nicht
- Sicherheitsvorkehrungen treffen !

Pictures: Private Archive M.Janke, P.Laackmann

Alpha Radiation Fault Angriffe
PROFESSIONELLE Beispiele

- Kalibrierte Strahlenquellen (z.B. Americium-241)
- “Geschlossene Strahler”, keine Kontamination
- Lokale Angriffe durch Maske auf Chipoberfläche, z.B. gegen RAM, Crypto-RAM, CPU, Crypto-Prozessor:
  - Kunststoff oder Lackbeschichtung
  - Löcher manuell, durch Laser oder Fotoprozess
  - Bestrahlung einzelner oder mehrerer Chipareale
  - Manuelle Mikropositionierung der Maske
- Professionelle Strahlenquellen sind teuer (ca.1000 Euro)
- Strahlenquellen werden üblicherweise nicht an Privatpersonen verkauft.
- Anwender muss eingewiesen sein und Sicherheitsvorkehrungen treffen.

Pictures: M.Janke/P.Laackmann (Infineon)

Alpha Radiation Fault Angriffe
AMATEUR Beispiele

- Haushalts-Strahlenquellen:
  - Radium-Uhrzeiger (Ra-226)
  - Uran- und Thorium-Mineralien (Ra-226, U-238, Th-232)
  - Glühstrümpfe für Gaslaternen (Th-232)
  - Rauchmelder (Am-241)

- Durch Maskierung des Chips lokalisierte Angriffe z.B. gegen RAM, CPU, Crypto-Module:
  - Plastik-Maske (z.B. Overhead-Folie)
  - Löcher mit heißer Nadel eingestochen
  - Folie direkt auf Chip platziert
  - Billig-Methode: „Nagellack“ o.ä.
  - Kerzenruß

- Vorsicht !
- Solche Strahler sind ungeschützt, Stärke oft unklar !
- Risiko der Kontamination !
- Rauchmelder nicht auseinandernehmen !

Pictures: Private Archive M.Janke, P.Laackmann

Alpha Radiation Fault Angriffe
GEEK Beispiel

- IDEE: Wir lassen mal einen modernen Smartcard Chip gegen die erste Atombombe antreten!
- „Trinitit“: Geschmolzener Sand von der Trinity Test Site
- Bei Mineraliensammlern bekannt
- Nicht als radioaktives Material klassifiziert
- Nach 68 Jahren nur noch sehr wenig Aktivität meßbar
- Glasartige Seite mit 1mm Abstand auf Chip aufgelegt
- Chip zeigt Effekte ! (aber erst nach langem Warten)

Pictures: Public Domain (left) and Private Archive M.Janke, P.Laackmann (right)

Security Nightmares:
Zweifelhafte Statements & „Security Bullshit Bingo“

Vorsicht bei Hersteller-Statements wie:

- „Attacks are impossible.“
- „We use hundreds of security features, therefore it cannot be attacked.“
- „It would take a million years to...“
- „Attacks will not work because we use the smallest technology nodes.“
- „That attack can not be done by a student.“
- „We did enhancements against *recent* attacks.“
- „We employ hundreds of the best security experts“
- „We use certification to make our products secure.“
- „You would need an *electron microscope* to do that.“
- Our top favorite: „Unclonable“ or „Unhackable“

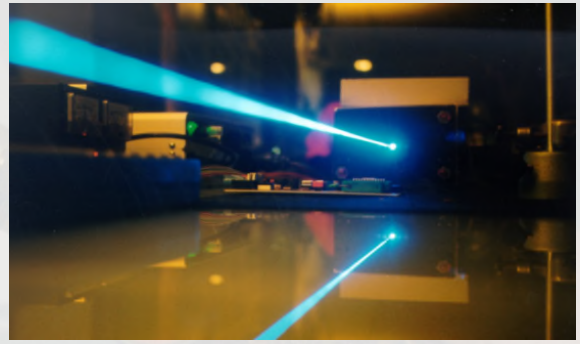
B	I	N	G	O
11	18	52	16	42
53	28	21	34	70
61	75	23	44	30
78	44	54	34	25
64	31	15	19	56

Security Nightmares: “Zertifizierungs-Detektoren” statt echter Sicherheit

- **Bei Autos (bereits bekannt):**
  - Es wurde von Autos berichtet, die speziell für den Verbrauchs-Test “optimiert” sind.
  - Sollen im Test deutlich weniger verbrauchen als im Real-Betrieb.

- **Bei Kühlschränken (bereits bekannt):**
  - Es wurde von Kühlschränken berichtet, die den Temperaturverlauf beim Test erkennen.
  - Werden Test-Bedingungen erkannt, werden Energieverbrauch&Kühlleistung gesenkt.
  - Sollen im Test deutlich weniger Energie verbrauchen als im Real-Betrieb.

- **Bei Security-Chips (noch nicht bekannt):**
  - Tests in der Sicherheits-Evaluierung sind de-facto Standard
  - Standard-Angriffsequipment ist verbreitet
  - Chips *könnten* Detektoren enthalten, die nur die Standard-Testumgebung oder Parameter erkennt und dann den Chip in Alarmzustand bringt. Chip wäre real unsicher !
  - Mögliches Beispiel: **„Laser Detectors“.**



Pictures: Private Archive M.Janke, P.Laackmann

Security Nightmares:
„Schlangen-Öl“ statt Sicherheit

„Schlangen-Öl“ Technologie kann gefährlich sein:

- „Unhackable“, „Unclonable“, „100% secure“, „Attack impossible“ evtl. Warnzeichen
- Kann mit “guter Story” hinterlegt sein
- Kann tatsächlich einen Angriff abwehren, gleichzeitig aber 10 andere erst ermöglichen.
- Kann vormals gut gesicherte Systeme völlig unsicher machen
- Kann Sicherheits-Evaluierungen in die Irre führen
- Kann mit schweren BACKDOOR Risiken verbunden sein…

So werden Physical „Unclonable“ Functions (PUF) zum HARDWARE-TROJANER

Security Nightmares:
Wie Vertrauenswürdig ist „Unclonable“ ?

Cloning Physically Unclonable Functions

Clemens Helfmeier*, Christian Boit
Semiconductor Devices,
Dept. of High-Frequency and Semiconductor System Tech.,
Technische Universität Berlin,
Berlin, Germany
{clemens.helfmeier,christian.boit}@.tu-berlin.de

Dmitry Nedospasov*, Jean-Pierre Seifert
Security in Telecommunications,
Dept. of Software Eng. and Theoretical Computer Science,
Technische Universität Berlin,
Berlin, Germany
{dmitry,jpseifert}@sec.t-labs.tu-berlin.de

* These authors contributed equally to this work

Abstract—As system security demands continue to evolve, Physically Unclonable Functions (PUFs) are a promising solution for secure storage on Integrated Circuits (ICs). SRAM PUFs are among the most popular types of PUFs, since they require no additional circuitry and can be implemented with on-die memories such as caches and data memory that are readily available on both ASICs and FPGAs. This work demonstrates that SRAM PUFs are not well suited as PUFs, as they do not meet several requirements that constitute an ideal PUF. The compact nature of SRAM, standard interconnects and resiliency to environmental effects make SRAM PUFs particularly easy to clone. We consider several ways in which SRAM PUFs can be characterized and demonstrate a Focused Ion Beam circuit edit with which we were able to produce a physical clone of our Proof-of-Concept SRAM PUF implementation. As a result of the circuit edit, when challenged, the physical clone produced an identical physical response to the original device. To the best of our knowledge, this is the first work in which a physical clone of a Physically Unclonable Function was produced.

I. Introduction

Secure storage is a critical component of any secure system and is often delegated to dedicated hardware. In many cases dedicated security Integrated Circuits (IC) are incorporated into the designs of secure systems specifically to take care of such tasks. Secret data can be programmed into a secure IC during production by the vendor or personalization by the end-user [1]. In systems lacking Non-Volatile Memory (NVM), key storage and distribution can be particularly difficult.

However, even with NVM, an attacker can utilize any number of techniques to read-out on-die memories [2]. One especially promising avenue to solve the problems of key storage are Physically Unclonable Functions (PUFs) since intrinsic process variations can be used to implement unique challenge/response pairs for every IC [3], [4]. When implemented correctly, a key does not have to be stored at all, but is instead derived from the characteristic response of a PUF. Ideally, the characteristic response changes whenever the IC is altered, i.e. when the device is depackaged. Such behavior provides an additional layer of tamper-resistance [5].

One of the most researched and popular classes of PUFs are memory-based PUFs [6]. Such PUFs utilize the settling state of volatile memory, such as Static Random Access Memory (SRAM), to implement unique challenge/response pairs. Such memories are already present on secure ICs and offer hardware vendors substantial flexibility during manufacturing. Memories can be partially or completely re-purposed to temporarily or permanently act as a PUF at startup. SRAM is commonly included in such solutions, making SRAM-based PUFs especially popular [7]. SRAM and SRAM-based PUFs are also particularly resilient to temperature variations and are generally more compact than many other memory-based PUFs [8].

Though several works to date have described the characteristics of an ideal PUF, this work focuses on the original definitions introduced in [3]. This work demonstrates that SRAM PUFs violate at least the following characteristics of an ideal PUF:

- **Manufacturer resistant** - It should be infeasible to create a second PUF that generates the same response.
- **Hard to characterize** - It should be infeasible to characterize the response of a PUF.
- **Controlled** - The PUF should be difficult to access for the attacker and implement some tamper-resistance.

The main contributions of this paper are: (1) *First successful physical clone.* We successfully reproduced the "unique" response of our Proof of Concept (PoC) SRAM PUF implementation in a second identical device. We used a Focused Ion Beam (FIB) circuit edit (CE) to produce a fully-functioning second instance of the device with an identical physical response to that of the target device. To the best of our knowledge this is the first successful hardware-based cloning attack against a PUF. (2) *Several strategies to read out SRAM.* If the entire contents of the SRAM can be extracted, an SRAM PUF can be fully-characterized. We review several techniques with which the contents of SRAM at startup can be extracted allowing an attacker to recover the unique response of the IC. (3) *Discussion and Countermeasures.* We discuss several inherent weaknesses of memory-based PUFs as compared to other classes of PUFs. We also introduce several mitigation techniques with which hardware vendors can make our attack significantly less cost-effective for the attacker.

The rest of this paper is structured as follows: In Section II we provide additional necessary background information on the 6T-SRAM cell circuit as well as SRAM PUF implementations. The FIB CE is explained in Section III. In Section IV we

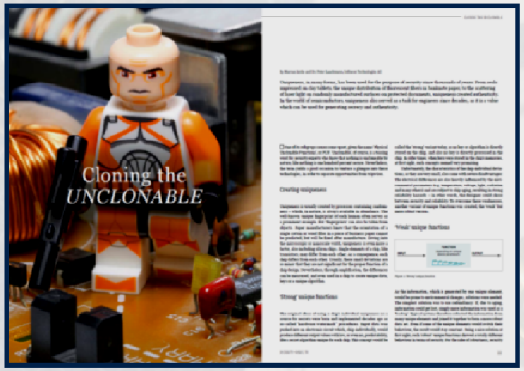
Attacks on PUFs [edit]

Proposed PUFs are not necessarily unclonable and many have been successfully attacked in a laboratory environment.[36]

Despite being named "physical unclonable", a research team from Berlin Institute of Technology was able to clone an SRAM university failure analysis labs.[36] In this work only srams cells of a microcontroller where read out.

From 2010 onwards till 2013, PUF gained attention in the smartcard market as a promising way to provide "silicon fingerprin individual smartcards.[37][38] However, university research has shown that delay-based PUF implementations are vulnerable

Source: Wikipedia



The amount of lab time necessary to produce an initial clone was about twenty hours, whereas subsequent clones can easily be produced in under three hours. Nevertheless, producing a

Hardware Trojan Side-Channels Based on Physical Unclonable Functions

Zheng Gong[1,*] and Marc X. Makkes[2]

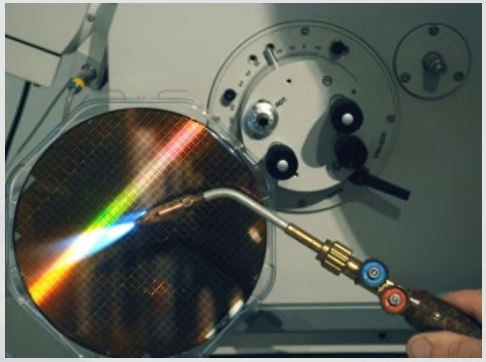
[1] School of Computer Science, South China Normal University
Guangzhou, 510631, China
cis.gong@gmail.com
[2] Eindhoven University of Technology
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
m.x.makkes@kr85.org

Abstract. The separation design and fabrication process in the semiconductor industry leads to potential threats such as trojan side-channels (TSCs). In this paper we design a new family of TSCs from physical unclonable functions (PUFs). In particular, a dedicated attack on the PRESENT block cipher is described by using our PUF-based TSCs. Finally we analyze the performance of our PUF-based TSCs and discuss other potential applications.

1 Introduction

“Der Elektronenstrahl”
Das Multi-Tool für den Angreifer

Elektronstrahlen können verwendet werden für:



• **Reverse Engineering** (REM/SEM – Elektronen-Mikroskopie)
→ Chipfunktionen, Schaltpläne des Chips, ROM Inhalt

• **Live Probing** (Voltage Contrast Visualization, EBAC)
→ Chip-interne Signale lesen (Speicherinhalt, CPU, Busse)

• **Kurzfristige oder dauerhafte Änderung von Chipcharakteristiken**
  • Erzeugung von Sekundärelektronen beim Auftreffen, diese verändern das Verhalten
  • Lokale Erzeugung von Röntgenstrahlung bei hohen Spannungen
→ Verändern von analogen Werten, PUF-Inhalten, Sensoren…

• **e-Beam Schreiben von Fotomasken**
→ Amateur-Lithographie auf der Chiprückseite – fortgeschrittenes Probing/Forcing

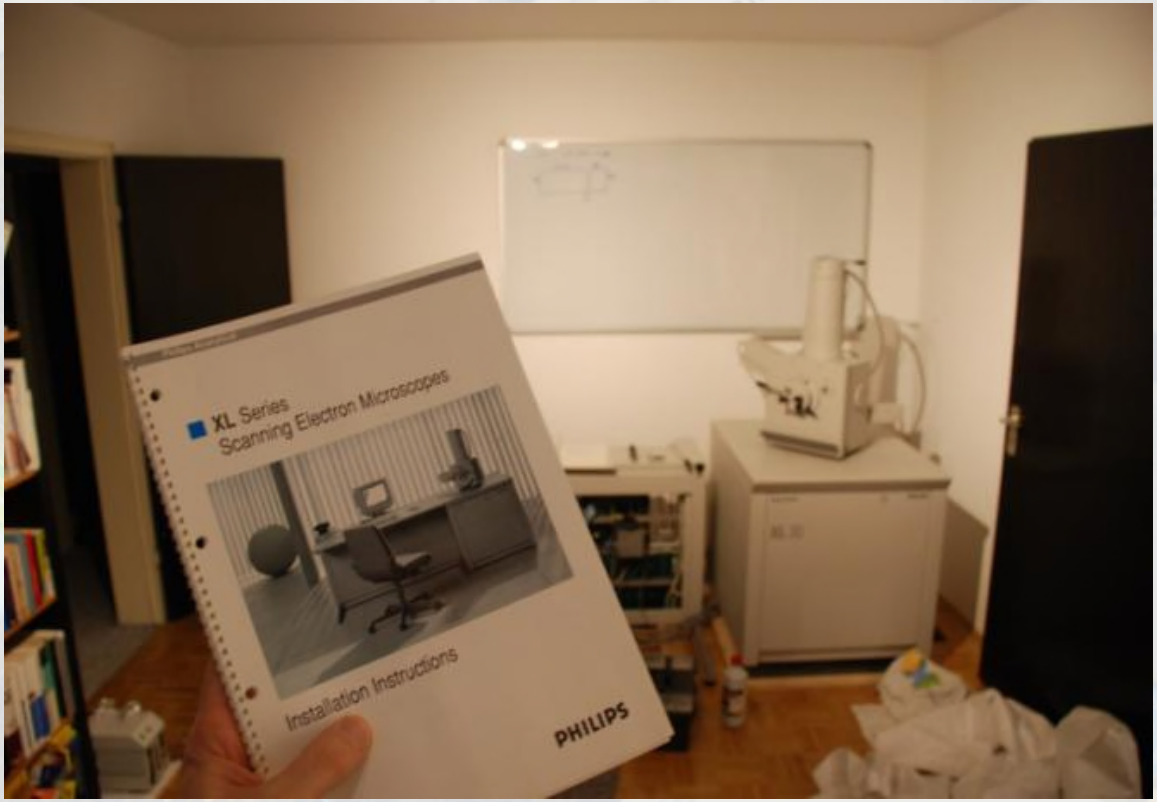
„Aber wer hat denn schon ein Elektronenmikroskop zu Hause?“*

1. Reserviere einen Platz im Wohnzimmer…

Pictures: Private Archive M.Janke, P.Laackmann

*Typisches Statement

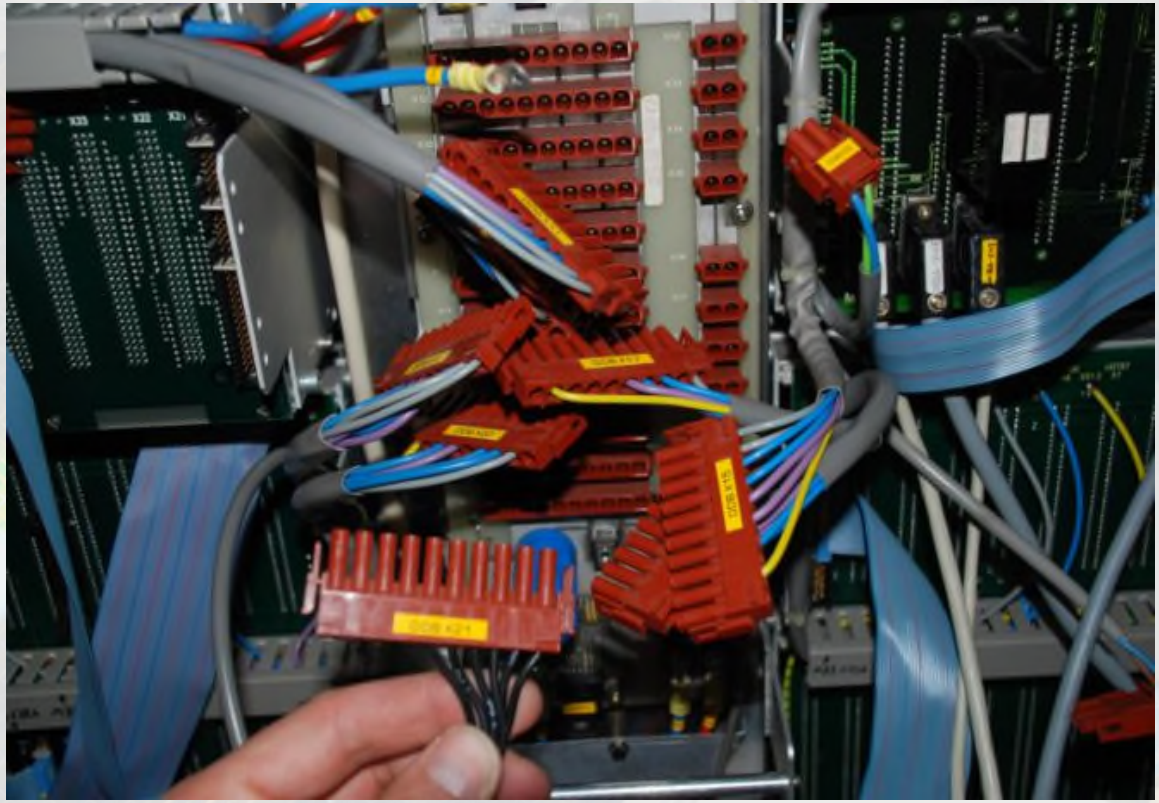
„Aber wer hat denn schon ein Elektronenmikroskop zu Hause?“



2. Lies das Manual

Pictures: Private Archive M.Janke, P.Laackmann

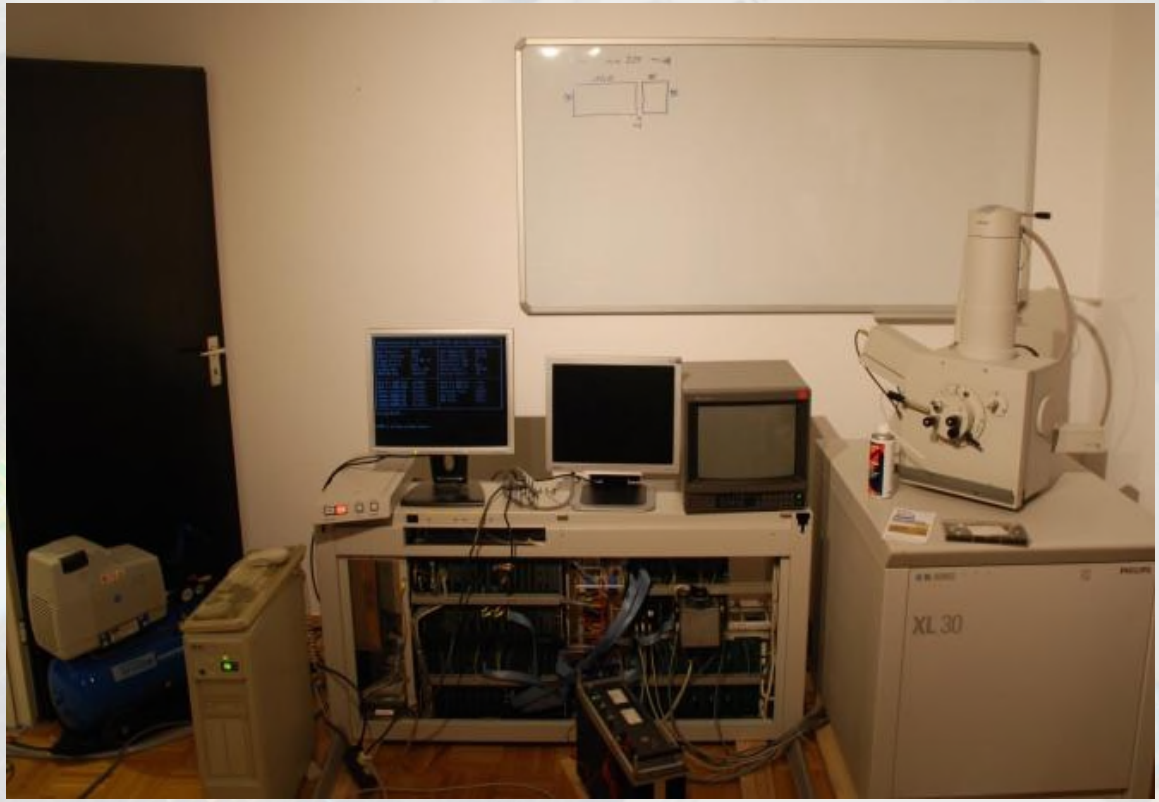
„Aber wer hat denn schon ein Elektronenmikroskop zu Hause?“



3. Verbinde dutzende Stecker für Strom, Wasser und Druckluft

Pictures: Private Archive M.Janke, P.Laackmann

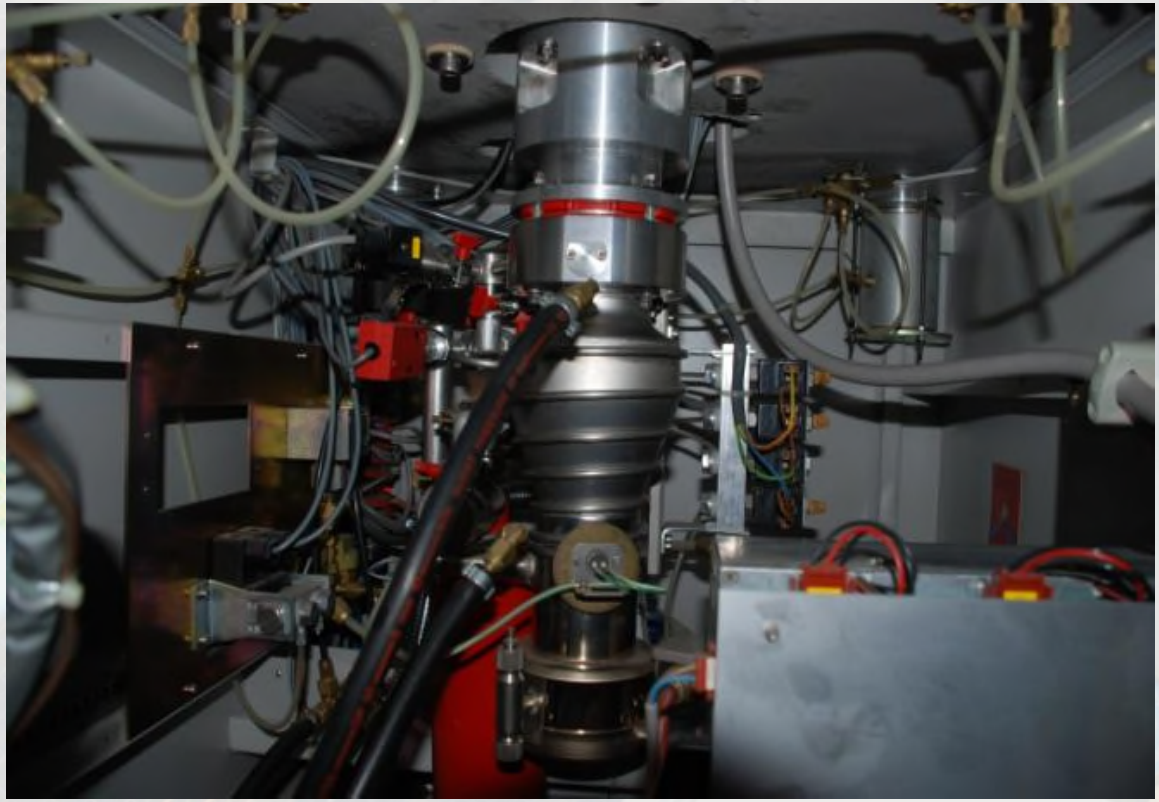
„Aber wer hat denn schon ein Elektronenmikroskop zu Hause?“



4. Bereite alles für den ersten Test vor

Pictures: Private Archive M.Janke, P.Laackmann

„Aber wer hat denn schon ein Elektronenmikroskop zu Hause?“



5. Teste das Vakuum System (Öl-Diffusionspumpe bevorzugt)

Pictures: Private Archive M.Janke, P.Laackmann

„Aber wer hat denn schon ein Elektronenmikroskop zu Hause?“

6. Benutze Gerät in ursprünglicher Konfiguration, oder…

Pictures: Private Archive M.Janke, P.Laackmann

„Aber wer hat denn schon ein Elektronenmikroskop zu Hause?“

7. Modernisiere es ein wenig.

Pictures: Private Archive M.Janke, P.Laackmann

Have Fun Researching

```
Article: 325 of de.org.ccc
Path: rztsun!Germany.EU.net!news.netmbx.de!news.Hamburg.Germany.EU.net
From: sleepadm@drdhh.hanse.de (CCC Schlafplatzorga)
Newsgroups: de.org.ccc,fido.ger.ccc
Subject: *** 9. CHAOS COMMUNICATION CONGRESS ***
Message-ID: <1992Dec15.062712.664@drdhh.hanse.de>
Date: 15 Dec 92 06:27:12 GMT
Organization: Digital Island
Lines: 77
Xref: rztsun de.org.ccc:325
```

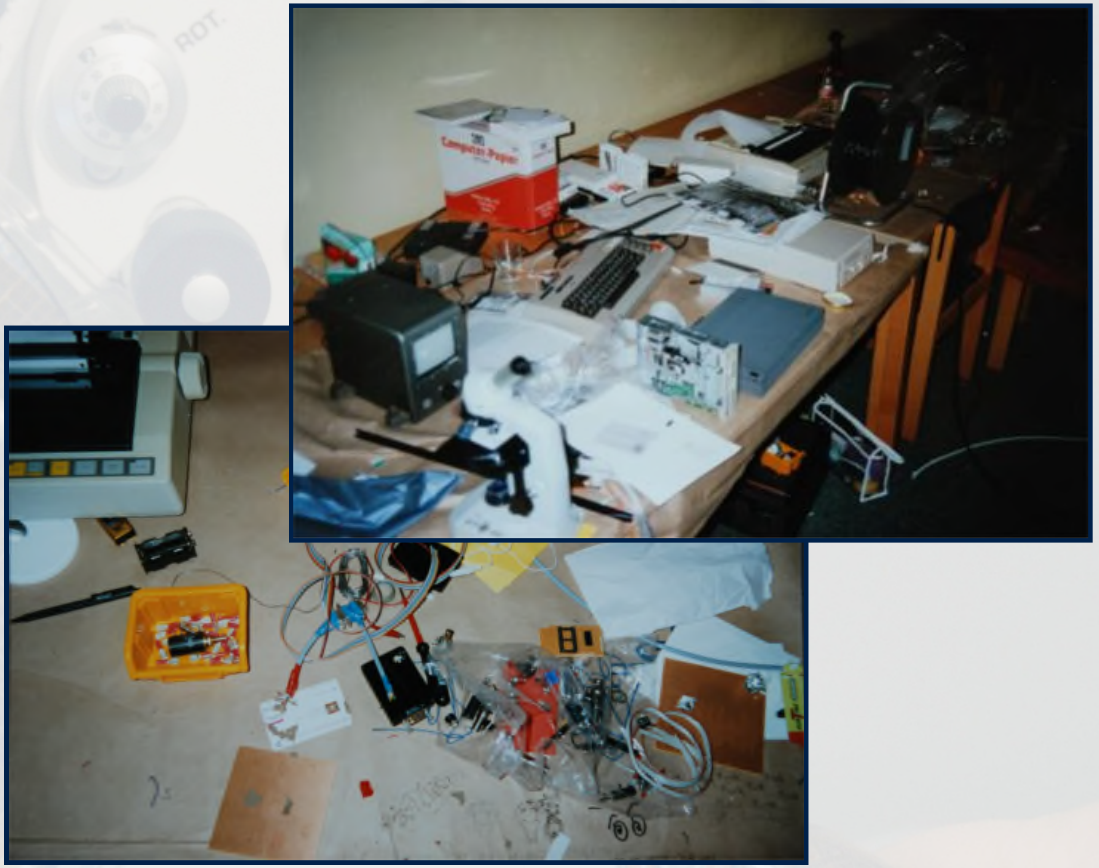
```
9. Chaos Communication Congress 1992
,,Es liegt was in der Luft''
,,There is something in the air''

27.12.1992 - 29.12.1992
Eidelst\"adter B\"urgerhaus
Elbgaustr. 12
D-2000 Hamburg 54
FRG
```

```
Other topics at the Chaos Communication Congress 1992 are:

Feminine computer usage - WOMEN ONLY !
How to use networks - Beginners
How to live with Networks - Semi-Professionals
How to live in Networks - Maniacs
Chip-Cards - Could you eat them ?
             What happened if you eat them with acid blobs ?
             What happened if you smoke them?

Prices: All three days: 36 DM (Members 26 DM)
```



Pictures: Private Archive M.Janke, P.Laackmann