

Attack Methodologies on Security Chips

Dr. Peter Laackmann
Marcus Janke



1989

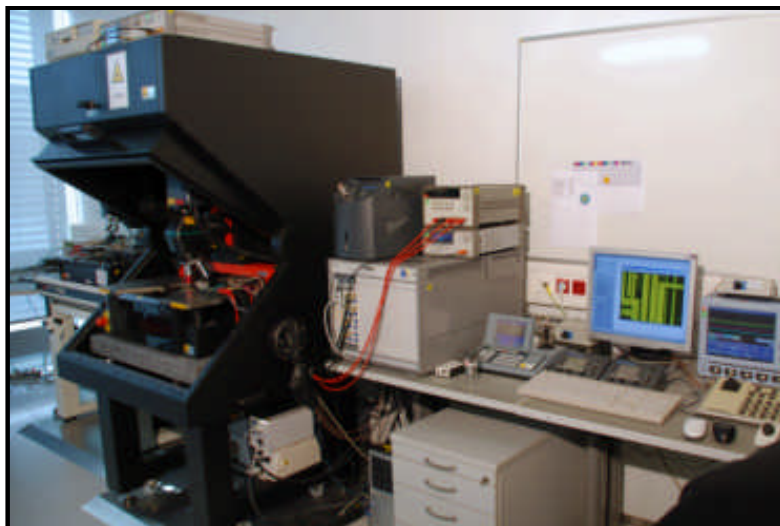
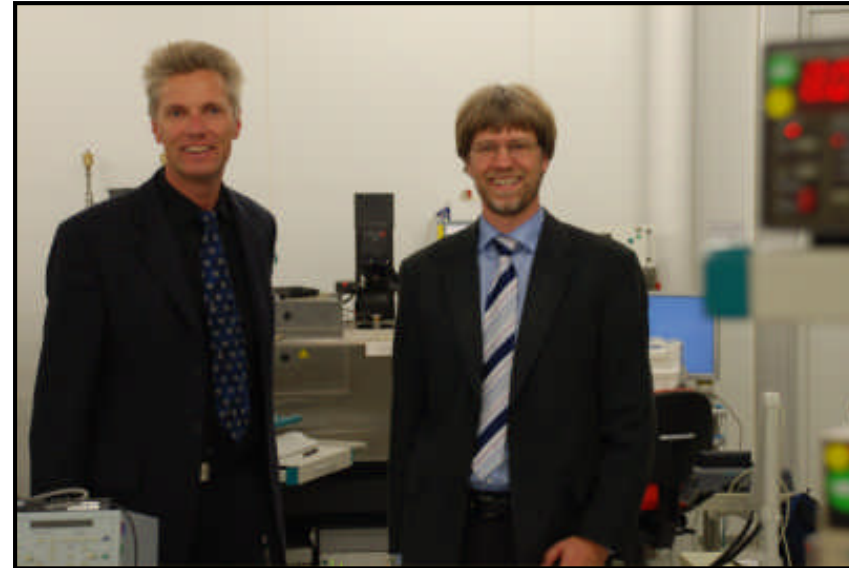
- Since 1989: Smart Card Research
- Brunsbüttel, Kiel, Hamburg
- Reverse Engineering
- Authors & Columnists during study
- Consultancy for Data Protection/Privacy
- Privacy/Security weaknesses revealed: Health insurance card, ec-card, ...
- Contacted by headhunter in 1999



Pictures: Private Archive M.Janke, P.Laackmann

2015

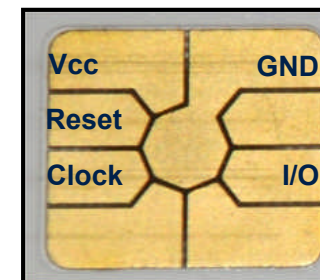
- Since 1999: Working with Infineon
- Munich
- Chip Security (Operational&Strategic)
- Leading the internal „hacker“ group
- Development of new attacks for threat anticipation
- Amateur attack projection
- Private security research ongoing...



Let's go 25 years back !

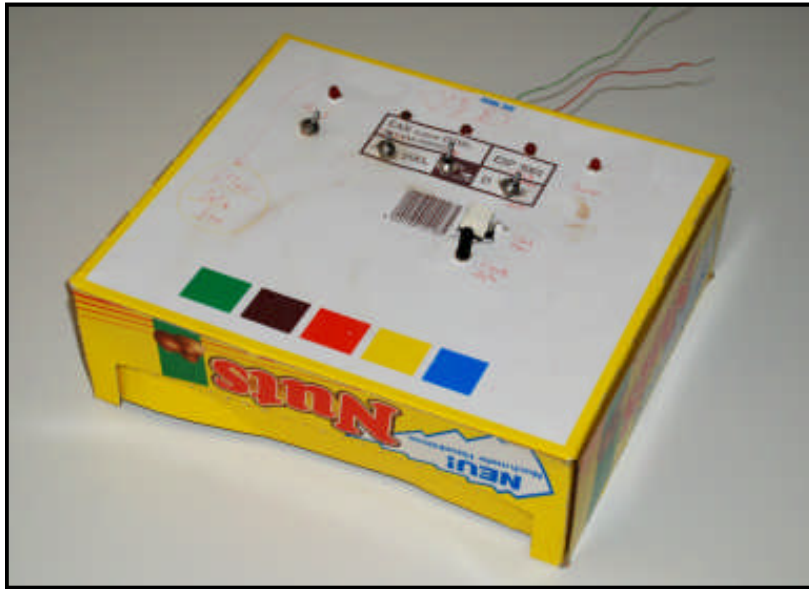


- Chipcards were NEW in the field
- Chip technology was unknown to public
- WHAT'S BEHIND THE GOLD CONTACTS?
- So let's do some reverse engineering! But...
- *Spent* cards were rare
- *New* cards were expensive (12 or 50 DM)
- Non-destructive analysis first, to save costs

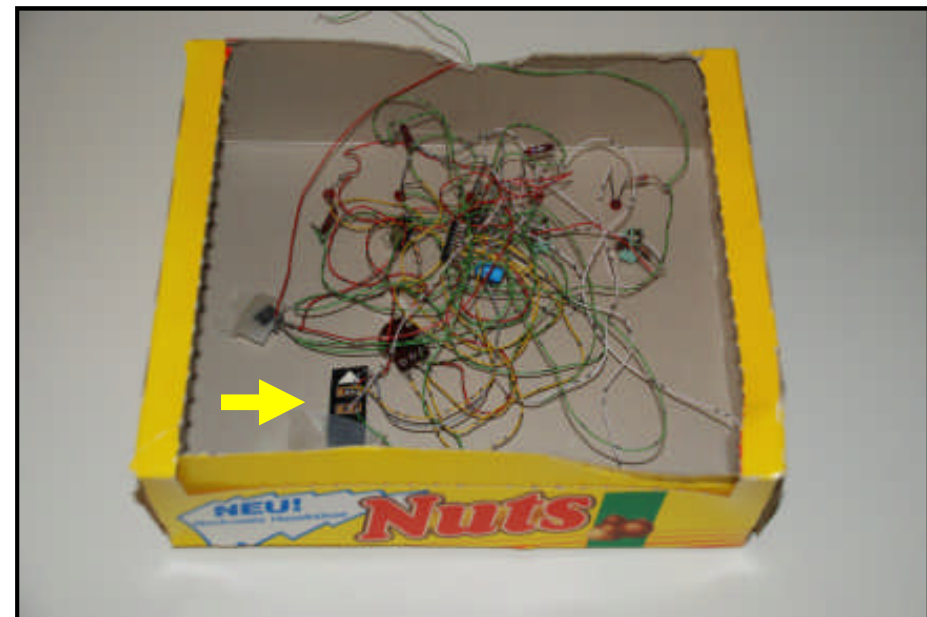


Pictures: Private Archive M.Janke, P.Laackmann

Let's go 25 years back !

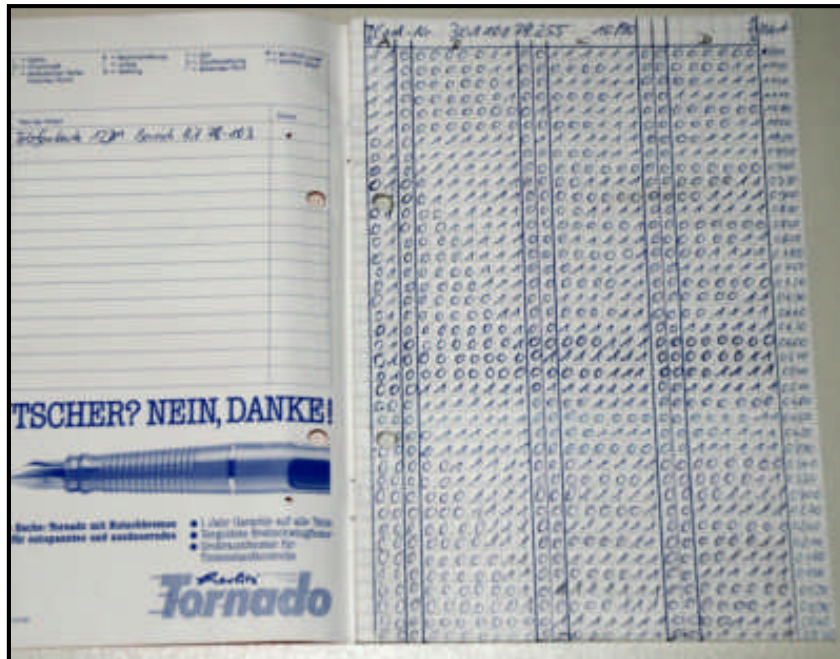


- Phonenumber functional analysis
- „Yellow Data Box“
- Contains phonenumber chip (see arrow)
- Stimulates Clock&Reset pins
- Shows phonenumber output (I/O)
- Logging done by pencil and paper...



Pictures: Private Archive M.Janke, P.Laackmann

Let's go 25 years back !

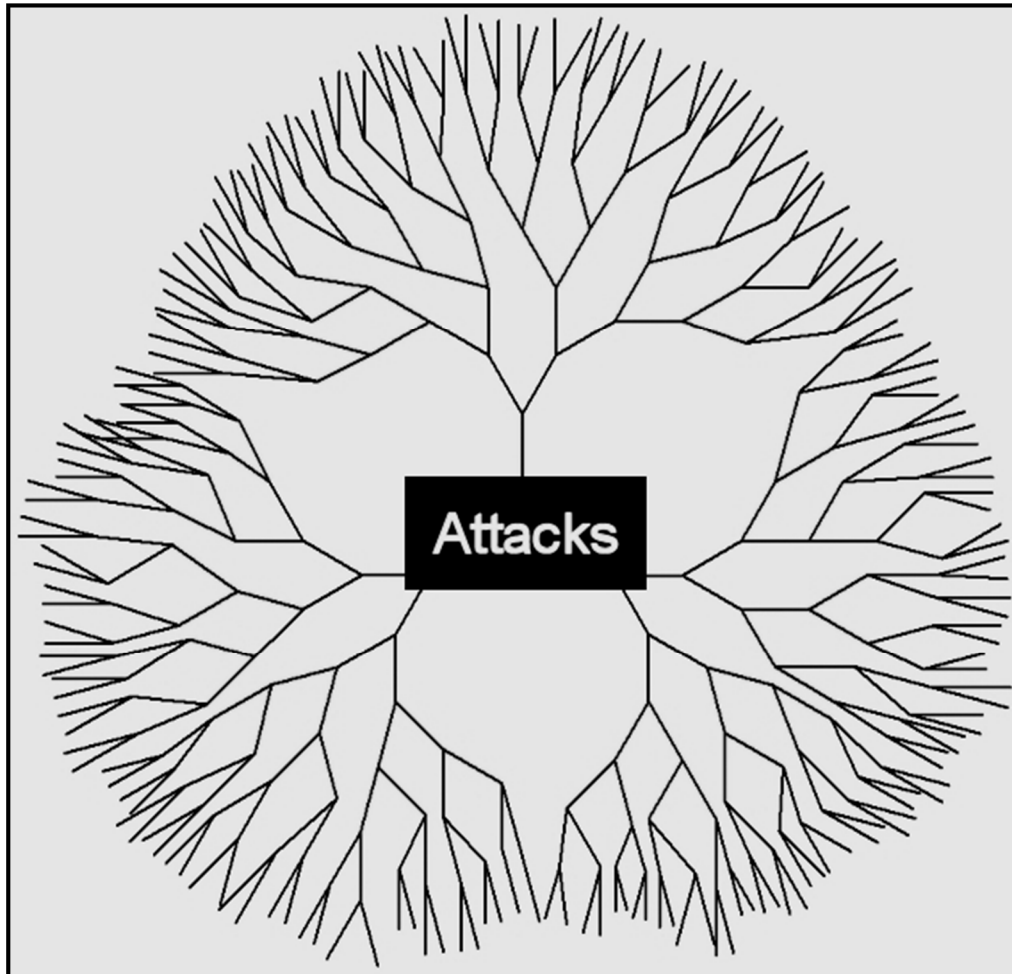


- Read one card after each of 40 units spent, 40 bicycle trips to cardphone needed...
- Intensive work on paper
- Next: Read different cards
- Compare bits to serial number, etc.
- Then: Automatic Readout with Commodore64 home computer
- Freeware published for C64 (64'er Magazin) and PC (C'T)



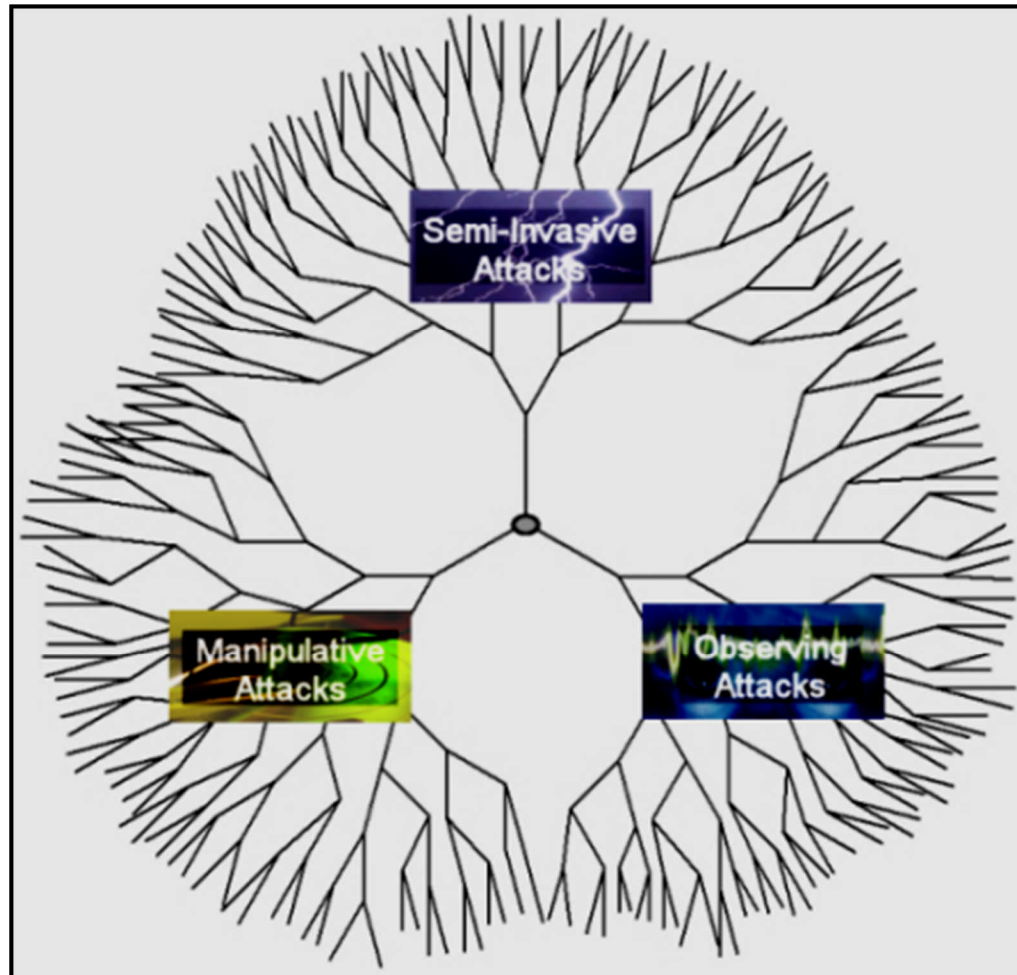
Pictures: Private Archive M.Janke, P.Laackmann

The „Attack Tree“ A Systematic Approach



- Today, many thousands of attack scenarios against smart card chips are known *and/or possible*.
- Visualisation: The „**Attack Tree**“, consists of branches, branchlets and leaves, like trees in nature.
- **Main branches** remain stable over time (attack classes)
- **Branchlets** change more often, get more, get bigger (attack groups)
- **Leaves** change very often, get more (specific attack scenarios)

The „Attack Tree“ A Systematic Approach



- **MANIPULATIVE Attacks**

- Probing, Forcing (Needles, AFM, FIB)
- Circuit Manipulation (FIB, Lasercutter)
- Destructive Reverse Engineering

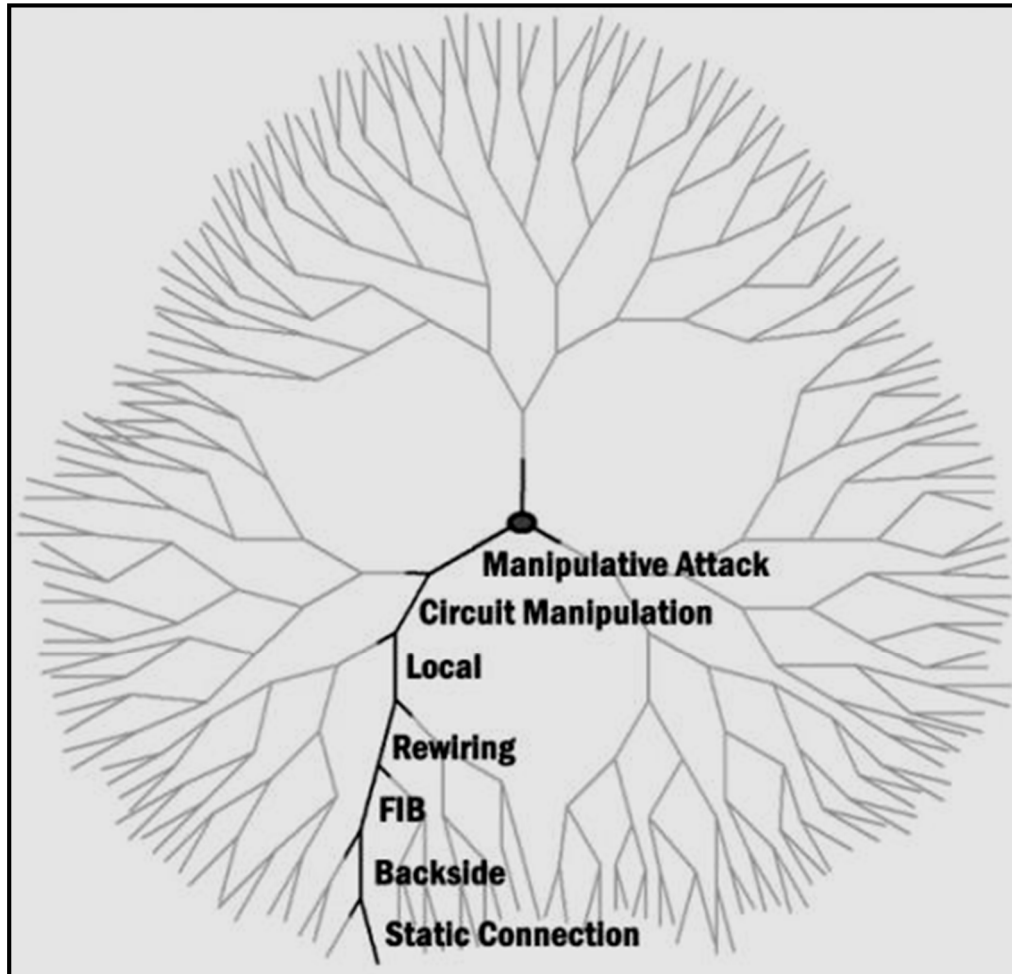
- **OBSERVING Attacks**

- Power Analysis (SPA, DPA)
- Electromagnetic Analysis (SEMA, DEMA)
- Optical Analysis (Optical Emission, OBIC, OBIRCH, LVP, Liquid Crystals)
- E-Beam, EBAC
- Timing Attacks (TA)
- Reverse Engineering (e.g. ROM readout)

- **SEMI-INVASIVE Attacks**

- Indirect Fault Induction (Spikes, Glitches, Laser, Alpha Radiation, X-Ray, Electron Beam, Heat/TIVA, Electric Field, Magnetic Field, electromagnetic induction and others)
- Direct Fault Injection (Signal Forcing by Needles, AFM, FIB, On-top-Lithography)

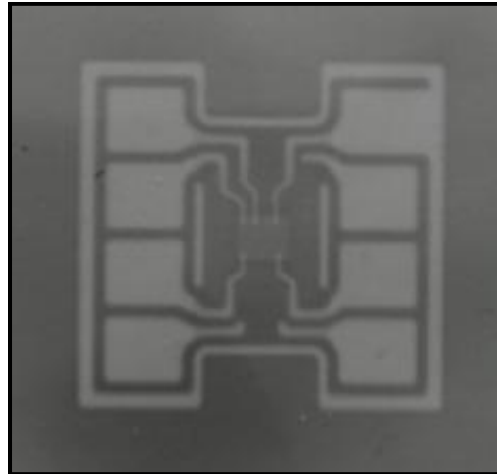
The „Attack Tree“ MANIPULATIVE Attacks



- Target of attack: Internal information to be revealed by electrical signal measurement or by optical inspection.
- Example for selection branch:
 - Circuit Manipulation vs. Reverse Engineering
 - Local vs. Chip global modification
 - Rewiring vs. Line-Cutting
 - FIB vs. Probing Needles
 - Backside vs. Frontside
 - Static vs. Changeable Connection
- “FIB” is just a small group in the class of “Manipulative Attacks”.
- A typical evaluation only covers a small subset of each group.

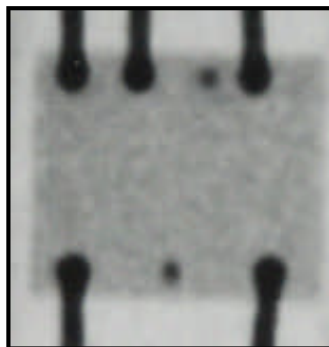
Manipulative Attacks

HISTORY Version

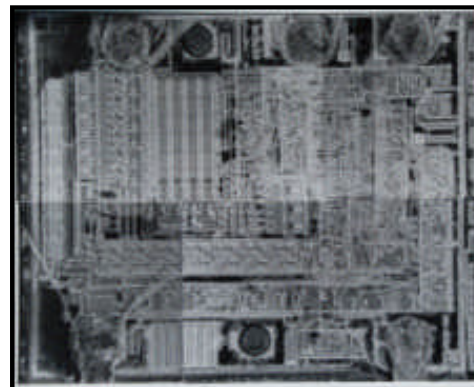


„TV-Set“ X-ray of phonecard

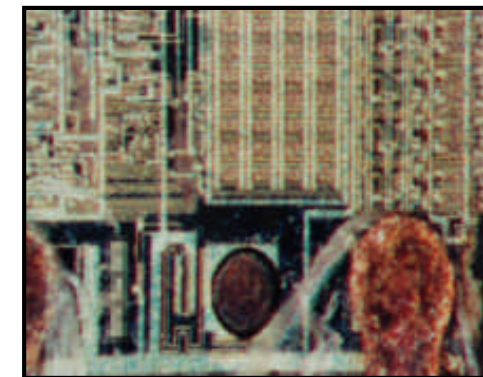
- X-Ray done inside old Color-TV set
- Exposure: Days to weeks
- No digital image processing available...
- Magnification & contrast by amateur photo lab
- Mechanical chip preparation
- Optical microscopy revealed details
- Test pads contacted and checked



Magnified negative shows additional pins on chip



Optical microscopy on black/white film



Optical microscopy, detailed on color film

Pictures: Private Archive M.Janke, P.Laackmann

Manipulative Attacks AMATEUR Version



Probing Station

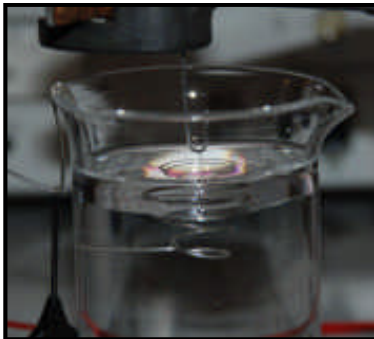
- Used equipment available at auctions
- Still fine for many smartcard security controllers



Selfmade Probing Needles

- Tungsten wire (e.g. wires from old light bulb, not the filament itself)
- Household chemicals: Sodium Hydroxide (drain cleaner), Ethanol, Benzine, Tensides (dishwashing)
- Electrochemical etching without process control gives 200nm needle tips
- Microprocessor controlled electrical etching gives extremely fine (down to 5nm) needle tips*

* 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.



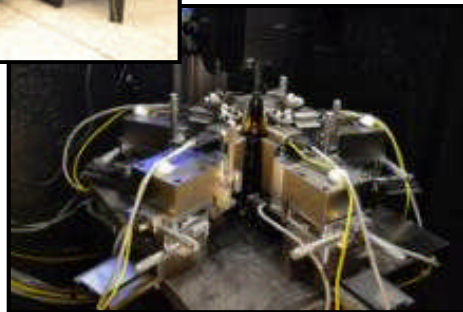
Atomic Force Microscope (AFM)

- Available as DIY kit for schools

Pictures: Private Archive M.Janke, P.Laackmann

Manipulative Attacks

PROFESSIONAL Version



Automatic Electron Microscope Chip Scanner

- Micropositioning stage with laser interferometer
- Positioning accuracy 50nm
- Generates image mosaic tiles and position data
- Analysis by specialized software

Focused Ion Beam (FIB)

- Backside/Frontside
- For all semiconductor technology nodes
- Milling, Insulator deposition, Contact deposition

Atomic Force Microscope (AFM)

- Detects „n” or „p” doped regions, read NVM cell
- Can be used for probing

µProbe Station

- <65nm direct probing

Manipulative Attacks

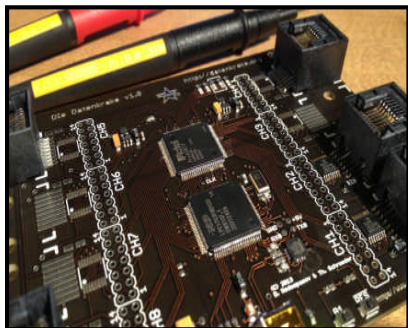
FUTURE Visions



Old Days

IDEA: „CHIP versus CHIP“

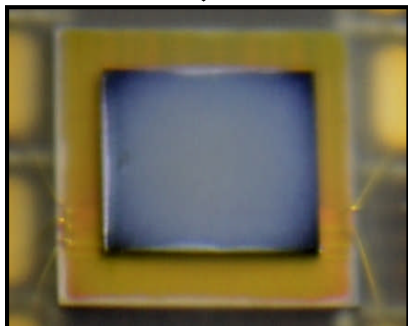
- Old days: Chip versus standard equipment (e.g. Oscilloscope)
- Today: Chip versus specialized equipment (e.g. „DDK“)
- Future: Chip versus Chip (e.g. specialized attack chip, mounted on the backside of victim chip)



Today

Realization: Lithography on backside

- Simple version: Apply signal lines on backside of victim chip
Needs photosensitive coating, e-Beam or laser writer, metallization and etching. Contacting with backside FIB
- Enhanced version: Apply FPGA on backside of victim chip
Needs customized rewiring on attack chip's surface to be connected to victim chip's FIB-prepared signals
- High-end version: Manufacture attack chip on backside of victim chip.
Needs sophisticated chip manufacturing equipment



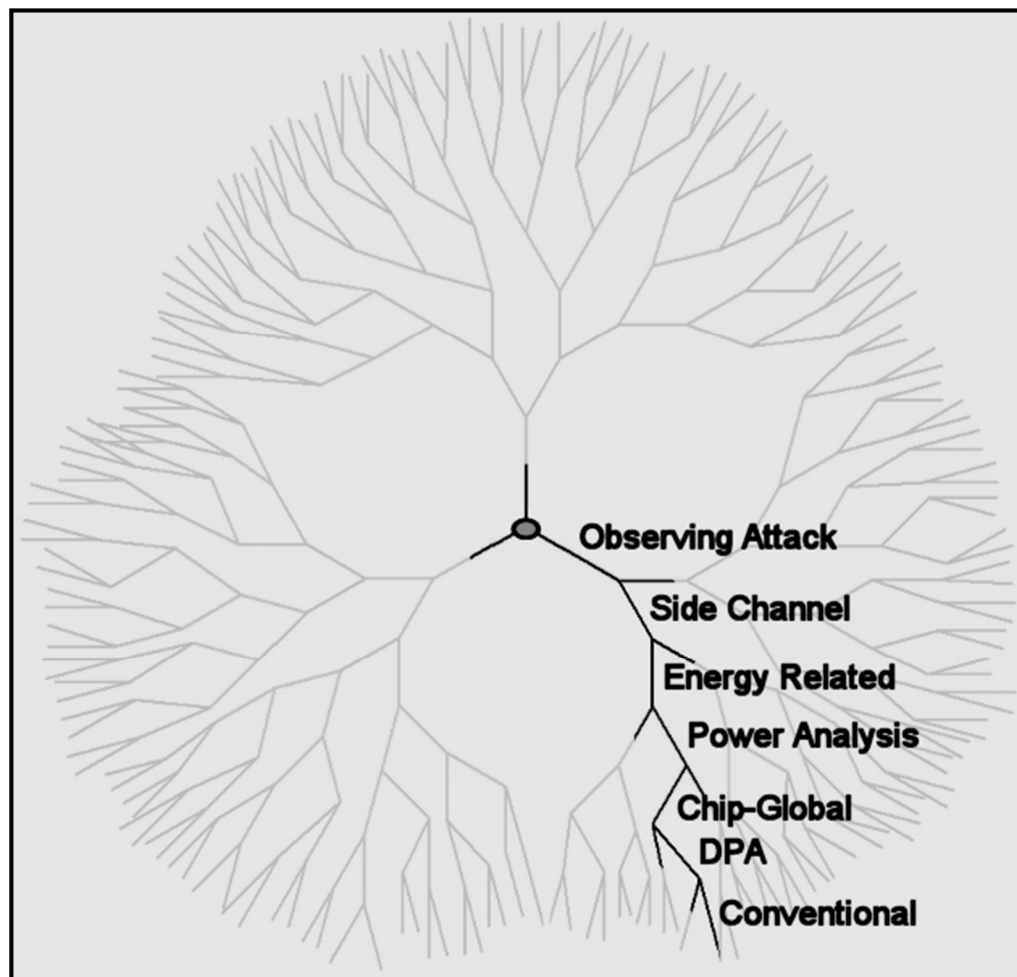
Future

Possibilities: Multi-probing and forcing in realtime

- Probing and forcing of multiple signals on the victim chip
- Real-time capabilities
- Signal amplification and level matching
- Signal conditioning and pre-processing

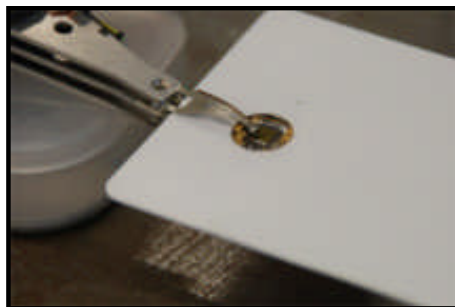
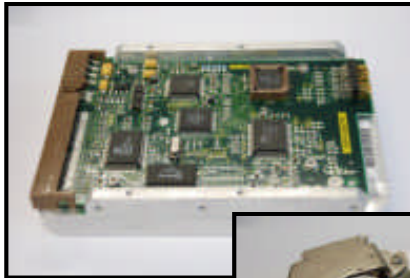
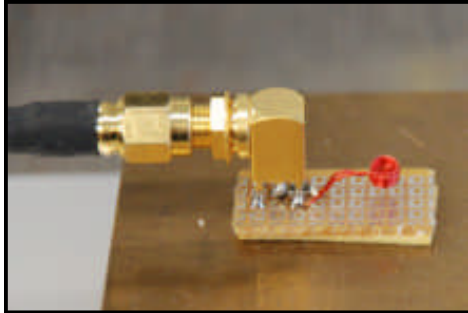
Pictures: Private Archive M.Janke, P.Laackmann (top, bottom) and D.Nedospasov (middle)

The „Attack Tree“ OBSERVING Attacks



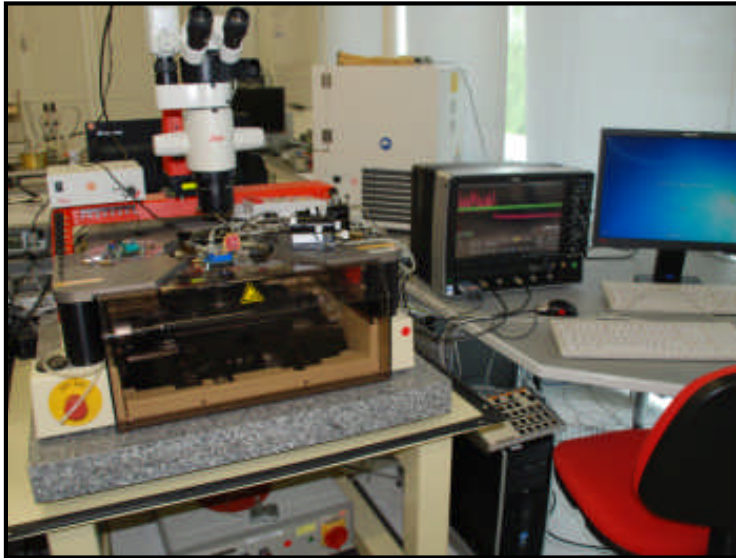
- Target of attack: Secret data like keys to be revealed by monitoring chip operation.
- Example for selection branch:
 - Side Channel vs. Direct Read-out
 - Energy Related vs. Timing
 - Power Analysis vs. Electro Magnetic Emission
 - Chip-Global vs. Local Measurement
 - DPA vs. SPA
 - Conventional vs. Advanced Postprocessing
- “DPA” is just a small group in the class of Side-Channel Attacks.
- A typical evaluation only covers a small subset of each group.

Electromagnetic Analysis AMATEUR Version

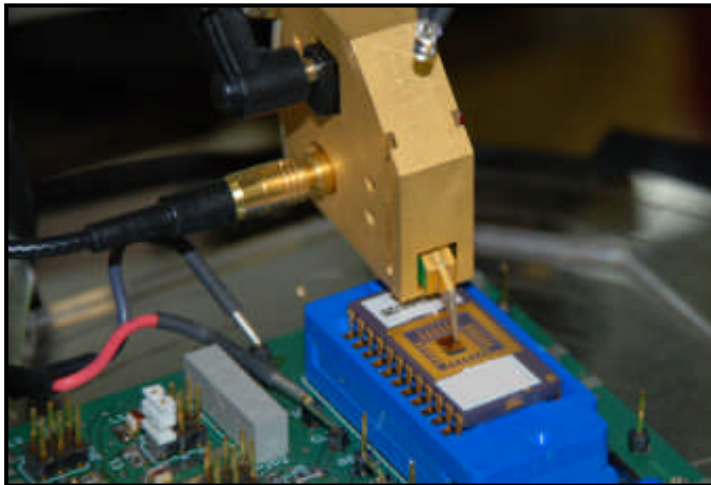


- Low-cost EMA probes:
 - Micro-coils from older harddrive sensor
 - Self-made copper wire coils
 - Ferrite probes
- Low-end digital oscilloscope
 - E.g. card for PC slot
 - USB oscilloscope
 - Low-end standalone oscilloscope
- PC harddrive for trace storage
 - 1-4 TB usual HDD
 - DPA freeware

Electromagnetic Analysis PROFESSIONAL Version

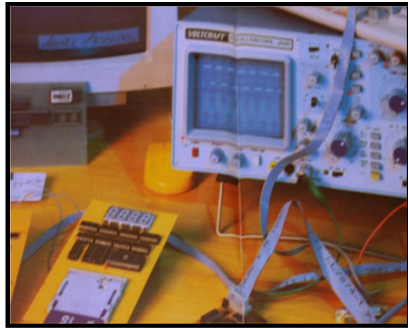


- Customized micro coil probe with internal low-noise GaAs amplifier
- Optional external GaAs amplifier
- Optional highpass/lowpass/band filter
- Signal logged on 40Gs/s oscilloscope
- Traces stored on 96TB RAID arrays
- Preprocessing
 - Digital frequency filtering
 - Signal timing alignment
 - Mathematics
- Mathematical Analysis of preprocessed digital signal for key recovery



Observative Attacks

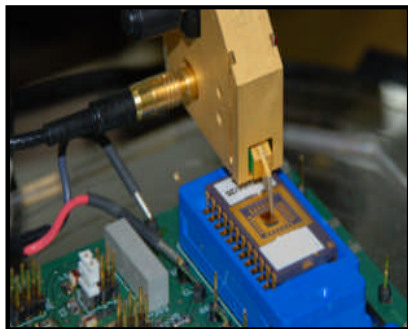
FUTURE Visions



Old Days

IDEA: „CHIP versus CHIP“

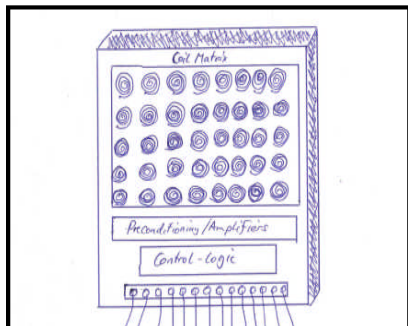
- Old days: Chip versus standard equipment (e.g. DPA with Oscilloscope)
- Today: Chip versus specialized equipment (e.g. „EMA microprobes“)
- Future: Chip versus Chip (e.g. specialized attack chip with EMA grid probes, backside IR contact imaging, OLED display-on-chip)



Today

Realization: Customized microchips

- EMA Grid: Customized chip with grid of microcoils (Coil-on-chip)
Coil-on-chip techniques commercially available, new layout needed.
- Backside IR contact imaging: Direct coupling of victim chip and imaging chip for photoemission analysis, possible combining with SIL (solid immersion lens).
Needs special optical design for SIL/chip combination.
- OLED display-on-chip: FIB-prepared backside signals are visualized with OLED coating on victim chip.
Needs coating equipment and some research.



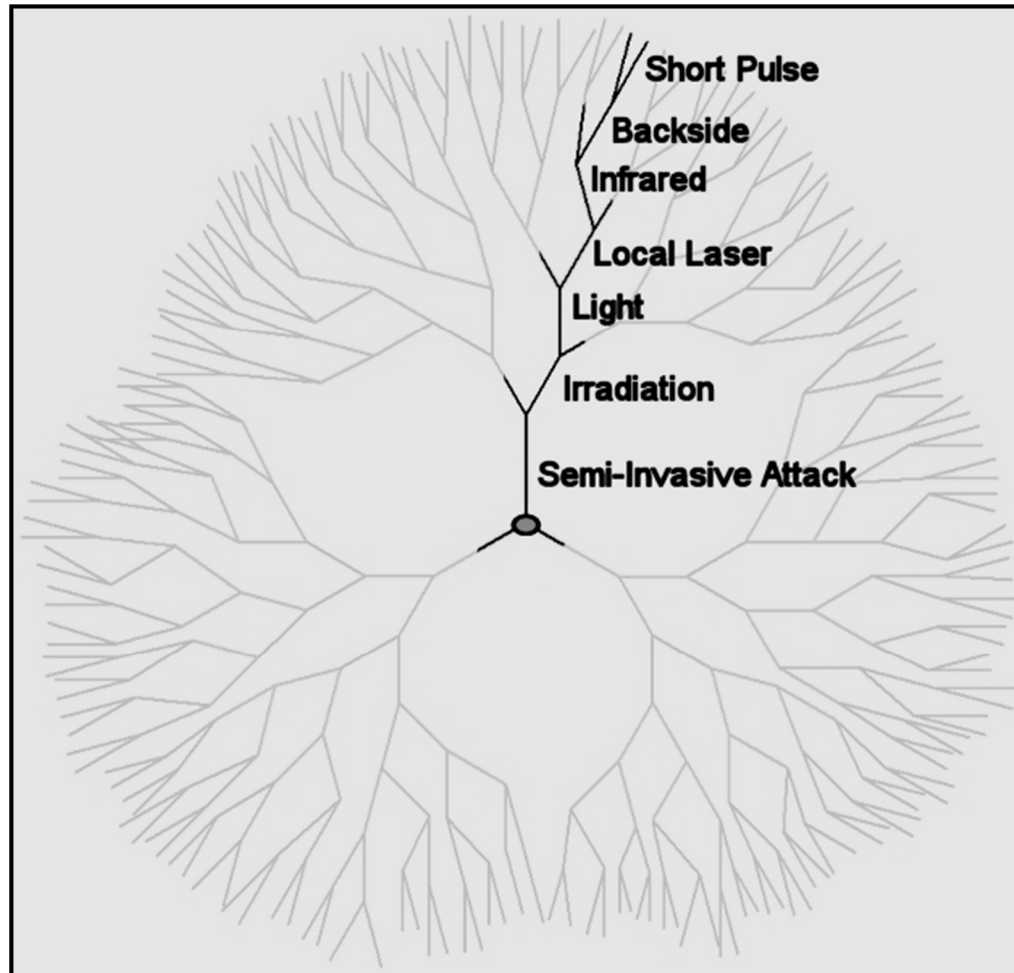
Future

Possibilities: Multi-signal observation on chip

- Observation of multiple signals on the victim chip
- Signal amplification and level matching (EMA grid-chip)
- Signal conditioning and pre-processing (EMA grid-chip)

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

The „Attack Tree“ SEMI-INVASIVE Attacks

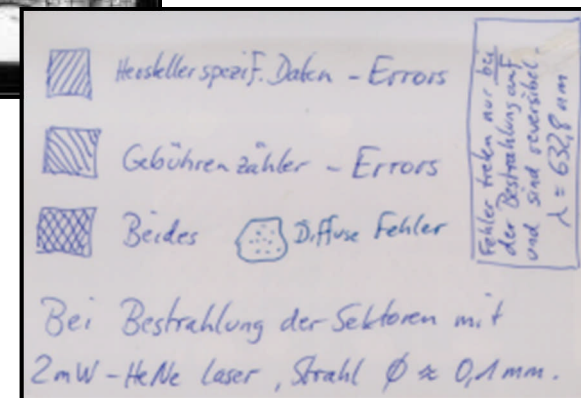
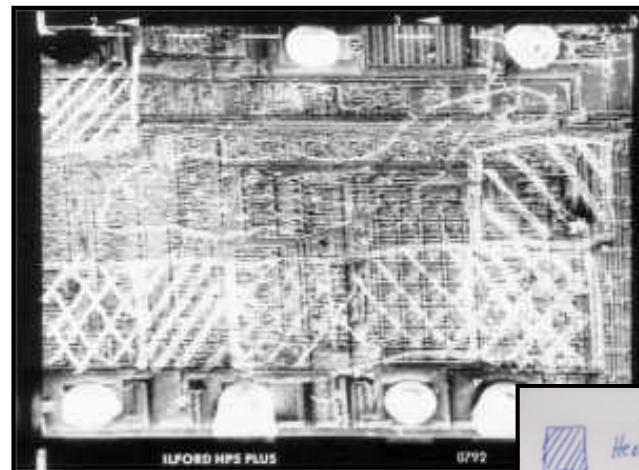


- Target of attack: Induction of errors in the program flow or in the processed data to gain secrets or circumvent software protection.
- Example for selection branch:
 - Irradiation vs. Power Supply changes
 - Light vs. Alpha Particle Irradiation
 - Local Laser vs. Global Illumination
 - Infrared vs. Green Light
 - Backside vs. Frontside Attack
 - Short Pulse vs. CW (Continuous Wave)
- “Laser Attack” is just a small group in the class of “Semi-Invasive Attacks”.
- A typical evaluation only covers a small subset of each group.

Optical Fault Induction HISTORY Version

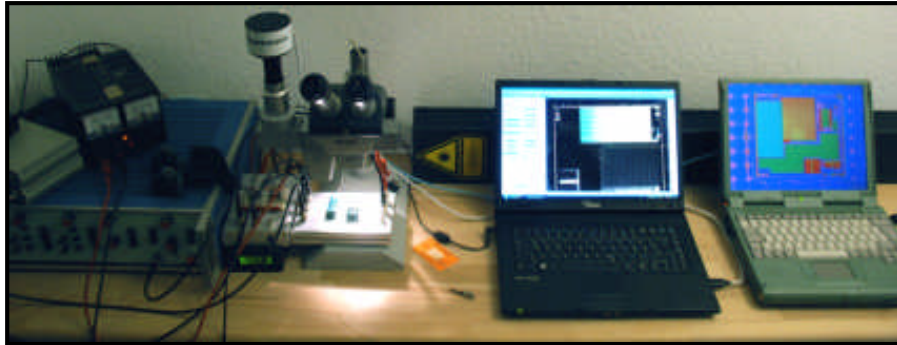


- 1992: We used a focused VideoDisc laser (HeNe tube) to induce errors on the chip for mapping chip functionalities.
- Identified general potential for targeted malfunctions (optical fault attacks).

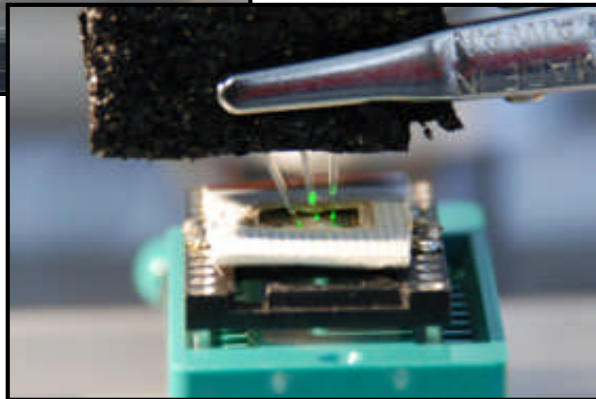
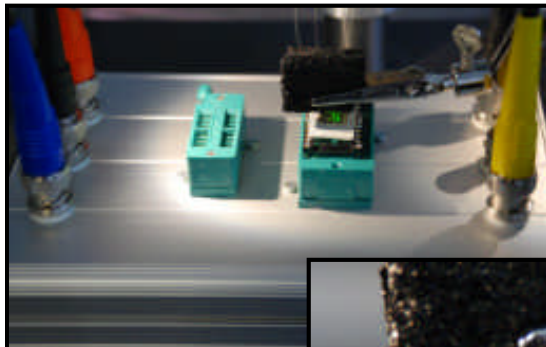


Pictures: Private Archive M.Janke, P.Laackmann

Optical Fault Induction AMATEUR Version



- Manual micropositioning
- Red or green laser (e.g. DPSS laser, China)
- Infrared lasers for backside attack
- Laser coupled into microscope camera input
- Option: Direct application via optical fibers
- Multi-spot attacks possible
- Laser triggered by software or FPGA
- 20kHz analog modulation is typical for low-cost lasers



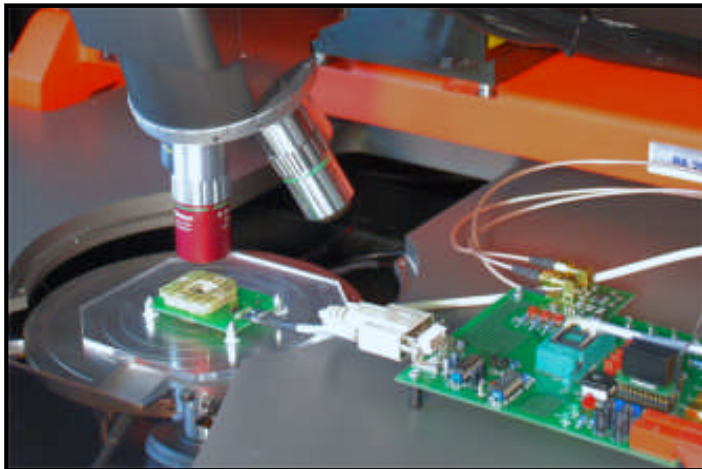
- **Warning: High-power lasers are dangerous**
- **Risk of severe eye damage – forever !**
- **All safety precautions have to be taken !**

Pictures: Private Archive M.Janke, P.Laackmann

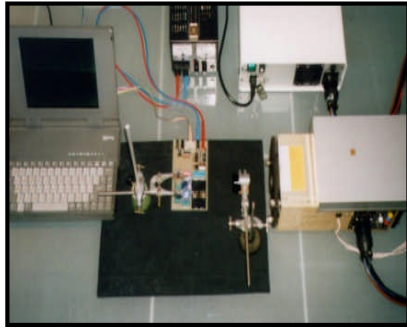
Optical Fault Induction PROFESSIONAL Version



- Automated chip scanning or manual option
- 3-axis motorized microprobing station
- Dynamic focussing via z-axis during scan
- Several wavelengths over UV, VIS, IR
- Backside and frontside attacks
- Backside IR imaging for navigation
- Multi-spot (area)
 - Mainly to attack (conventional) hardware and software security features
- Multi-shot (timing)
 - Mainly to attack software security
- Combination options (hybrid attacks)
 - Very powerful !



Optical Fault Induction FUTURE Visions



Old Days

IDEA: „CHIP versus CHIP“

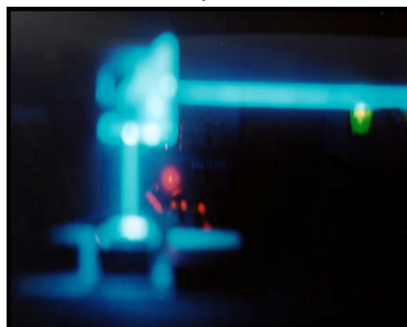
- Old days: Chip versus standard equipment (e.g. Laser on Microscope)
- Today: Chip versus specialized equipment (e.g. Multi-Laser Attack)
- Future: Chip versus Chip (Multiple-time, Multiple-area Laser Attack)



Today

Realization: Digital Light Processing / Spatial Modulators

- DLP Laser combination: Laser beam is modulated in time and space by array of DLP mirrors (like in projectors/"beamers")
Needs special setup and ideally special DLP arrays (capable for high laser energy levels)
- Spatial Modulators: Dynamic holographic light modulation with specialized equipment.
Needs special optical design.
- Concepts to manage large parameter variety are required.



Future

Possibilities: Multiple-area and multiple-time fault injection

- To attack many types of software countermeasures.
- To attack some types of hardware-countermeasures.
- Fast mapping of chip security features.

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

Alpha Radiation Fault Attacks AMATEUR Version



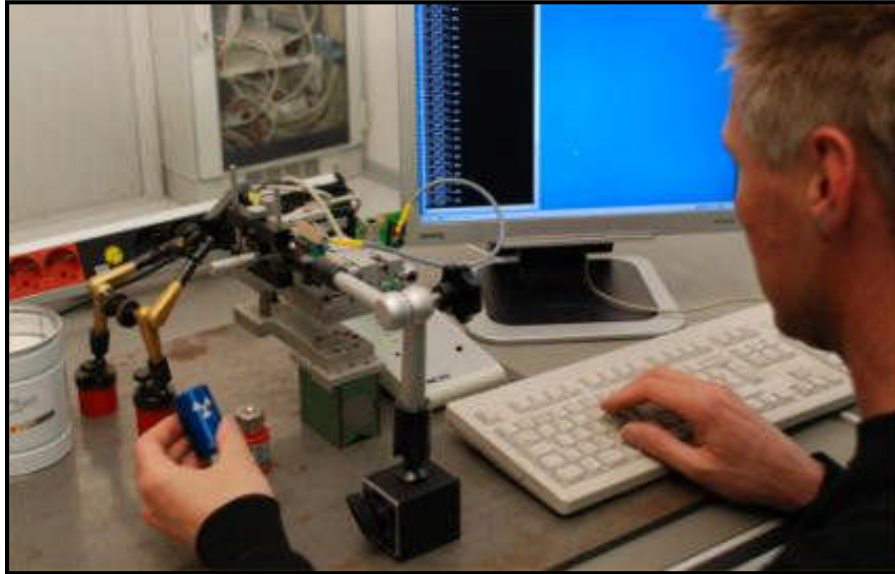
- Household radiation sources:
 - Old luminous Radium Dials (Ra-226)
 - Radioactive minerals (Ra-226, U-238, Th-232)
 - Old gas lantern mantles (Th-232)
 - Smoke detector sources* (Am-241)
- Localized attacks by radiation blocking e.g. against RAM, CPU, crypto-coprocessors:
 - Plastik mask (e.g. overhead slide)
 - Holes punched in mask (hot needle)
 - Mask placed directly on chip surface
 - Low-end method: „Nail Varnish“



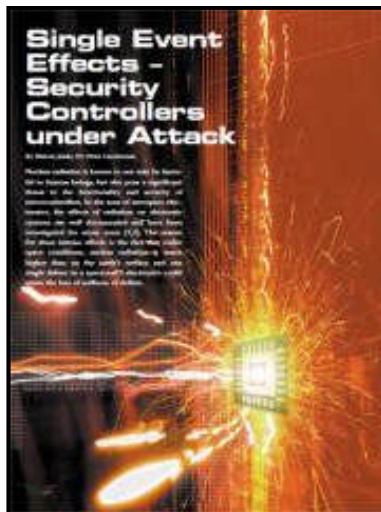
- **Warning !**
- **Such sources are not sealed, activity unknown !**
- **Risk of contamination !**
- **Do not disassemble radioactive smoke detectors !**

Pictures: Private Archive M.Janke, P.Laackmann

Alpha Radiation Fault Attacks PROFESSIONAL Version



- Calibrated sources (e.g. Am-241)
- Sealed sources, well secured for use
- Localized attacks by radiation blocking e.g against RAM, Crypto-RAM, CPU, crypto-coprocessors:
 - Plastic mask
 - Holes by punching, laser or photomask
 - Irradiation on multiple selected areas in parallel
 - Manual micropositioning of mask
- Expensive radiation sources (about 1-2k Euro)
- Radiation sources usually not sold to private persons
- **Personnel must be trained**

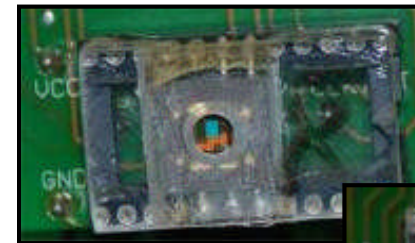


Alpha Radiation Fault Attacks

GEEK Version

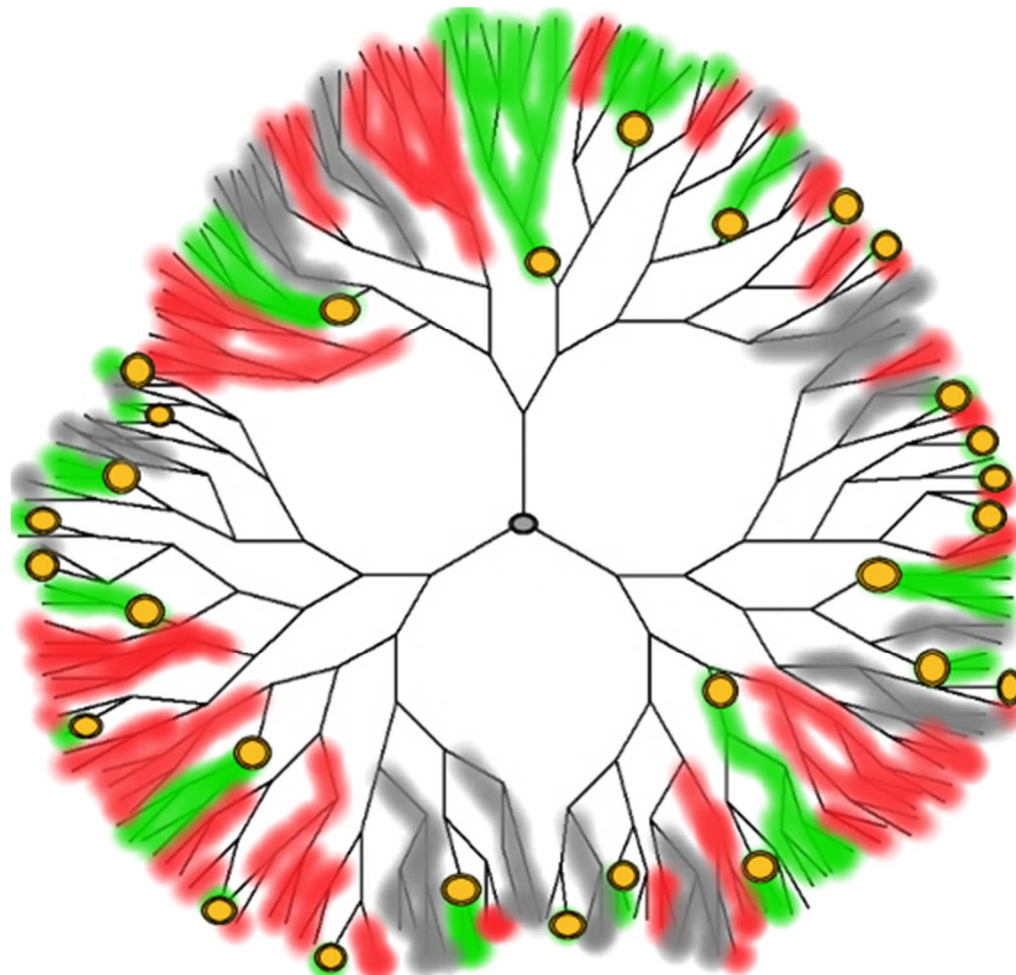


- IDEA: Let's use the first atomic bomb to test a modern smart card controller !
- „Trinitite“: Molten sand from test site (Trinity Site, New Mexico)
- Still available for mineral collectors
- Not specified as radioactive material
- Small level of alpha radiation (Am-241)
- „Glassy“ side placed down on chip
- Successfully generated effects on chip, but (of course) less than with usual sources

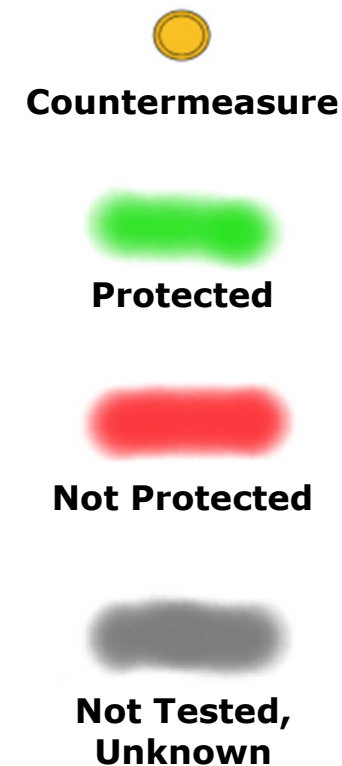


Pictures: Public Domain (left) and Private Archive M.Janke, P.Laackmann

The „Attack Tree“ An Exemplary View for Conventional Security



- Typical countermeasures are targeting small attack subsets only.
- Many countermeasures (yellow dots) are needed, many weaknesses remain.
- Many attack paths remain untested.



Security Nightmares: Doubtful Statements-„Security Bullshit Bingo“



Doubtful security statements can still be found in the market:

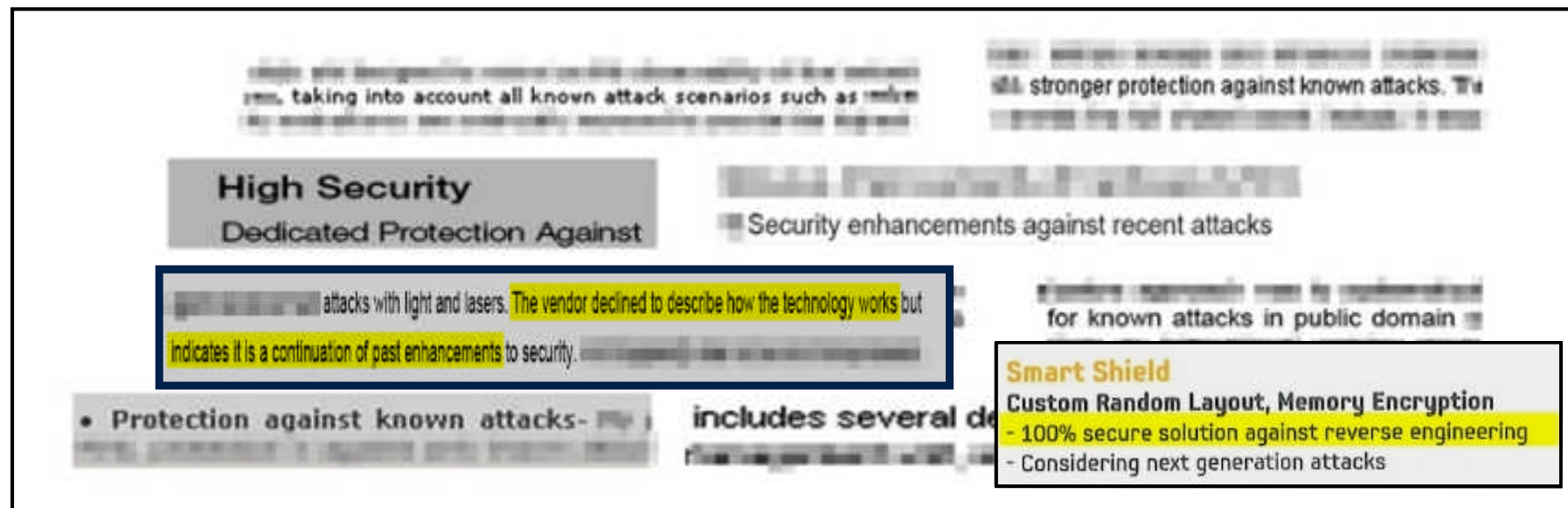
- „Attacks are impossible.“
- „Unclonable“, „Unhackable“
- „We use [*three-digit number*] security features, therefore it cannot be attacked.“
- „It would take [*number*] million years to...“
- „It is tamper-proof“
- „You would need an [*FIB, REM, ...*] to do that.“
- „Attacks will not work because we use the smallest technology nodes“
- „That attack can not be done by a student.“

BINGO				
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: „Warning Signs“ may Indicate Problems

Watch out for strange statements in the market:

- „100 Percent security“
- „We have an [*the attack you just asked for*] detector.“
- „Our engineer had a good idea during [*chose activity*]...“
- „We use certification to *make* our products secure.“
- „We did enhancements against *recent* attacks.“
- „We employ [*three-digit number*] of the best security experts“



The screenshot shows a webpage for a security product. Several text elements are highlighted with yellow boxes:

- A box containing the text: "attacks with light and lasers. The vendor declined to describe how the technology works but indicates it is a continuation of past enhancements to security."
- A box containing the text: "Stronger protection against known attacks. The..."
- A box containing the text: "Smart Shield Custom Random Layout, Memory Encryption - 100% secure solution against reverse engineering - Considering next generation attacks"

Other visible text on the page includes "High Security Dedicated Protection Against", "Security enhancements against recent attacks", and "Protection against known attacks-".

Security Nightmares: „Certification Detectors“ Instead of Security

- **Cars (reported):**

- Reports: Some cars are „optimized“ for known standard cycle test
- Emissions or fuel consumption in practice is higher

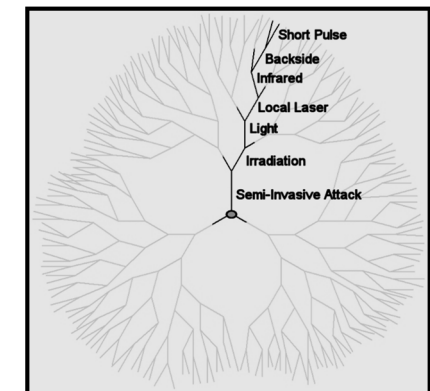
- **Fridges (reported):**

- Reports: Some fridges detect test conditions due to external temperature change
- Internal microcontroller shuts down cooling, simulates low energy consumption
- Power consumption in practice is much higher



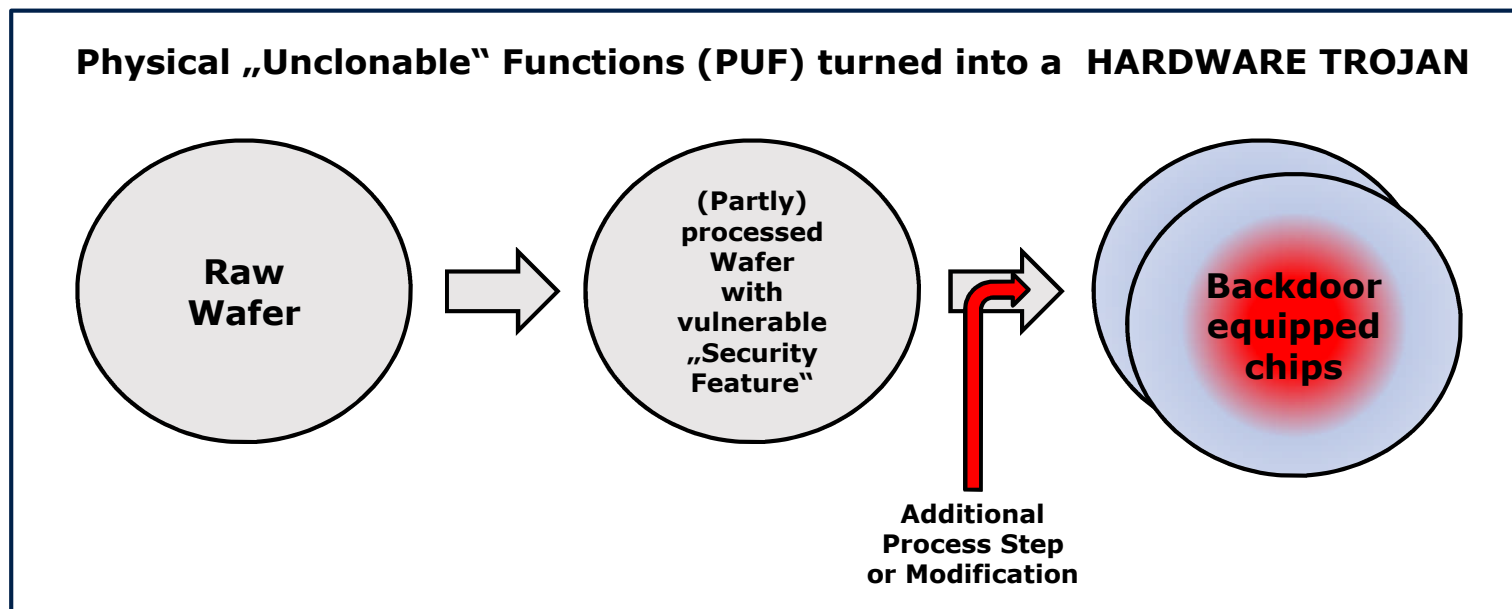
- **Security Chips (not yet reported):**

- Security evaluation uses very specific attack scenarios
- Standard attack equipment is commercially available and known
- There are indications that security features could be used to detect „certification environment“ rather than counteracting real attacks
- Inferior products could pass certification but fail in the field
- Example: „**Laser Detectors**“



Security Nightmares: „Snake Oil“

- **„Snake Oil“ security promises may be very dangerous**
 - „Unhackable“ technology, „Unclonable“ chips, „100% secure“, „Attack impossible“
 - Often „nice story“ for customers and end-customers, but:
 - May close one door for an attacker, while open ten others
 - May turn „quite secure“ systems totally insecure due to unforeseen threats
 - Sometimes, comes with severe BACKDOOR options...



Security Nightmares: „Unhackable“ or „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.^[30]

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 were read out.

From 2010 onwards till 2013, PUF gained attention in the [smartcard](#) market as a promising way to provide “silicon fingerprint” individual smartcards.^{[37][38]} However, university research has shown that delay-based PUF implementations are vulnerable

Source: Wikipedia



Hardware Trojan Side-Channels Based on Physical Unclonable Functions

Zheng Gong^{1,*} and Marc X. Makkes²

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



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

semi-physical on the SCs. Discuss

The Electron Beam

A Versatile Amateur Tool



An Electron Beam can be used for:

- **Reverse Engineering** (REM/SEM – Raster/Scanning Electron Microscopy)
 - Reveal chip function, schematics, ROM content
- **Live Probing** (Voltage Contrast Visualization, EBAC)
 - Read signals on chip (memory content, CPU operations, buses)
- **Temporary or Permanent variation of chip characteristics**
 - Localized secondary electron generation on impact
 - Localized X-ray generation on impact at higher acceleration voltages
 - Change memory or PUF contents, analog characteristics, sensor values...
- **e-Beam photomask writing**
 - Amateur lithography on the back side of the chip – advanced probing/forcing

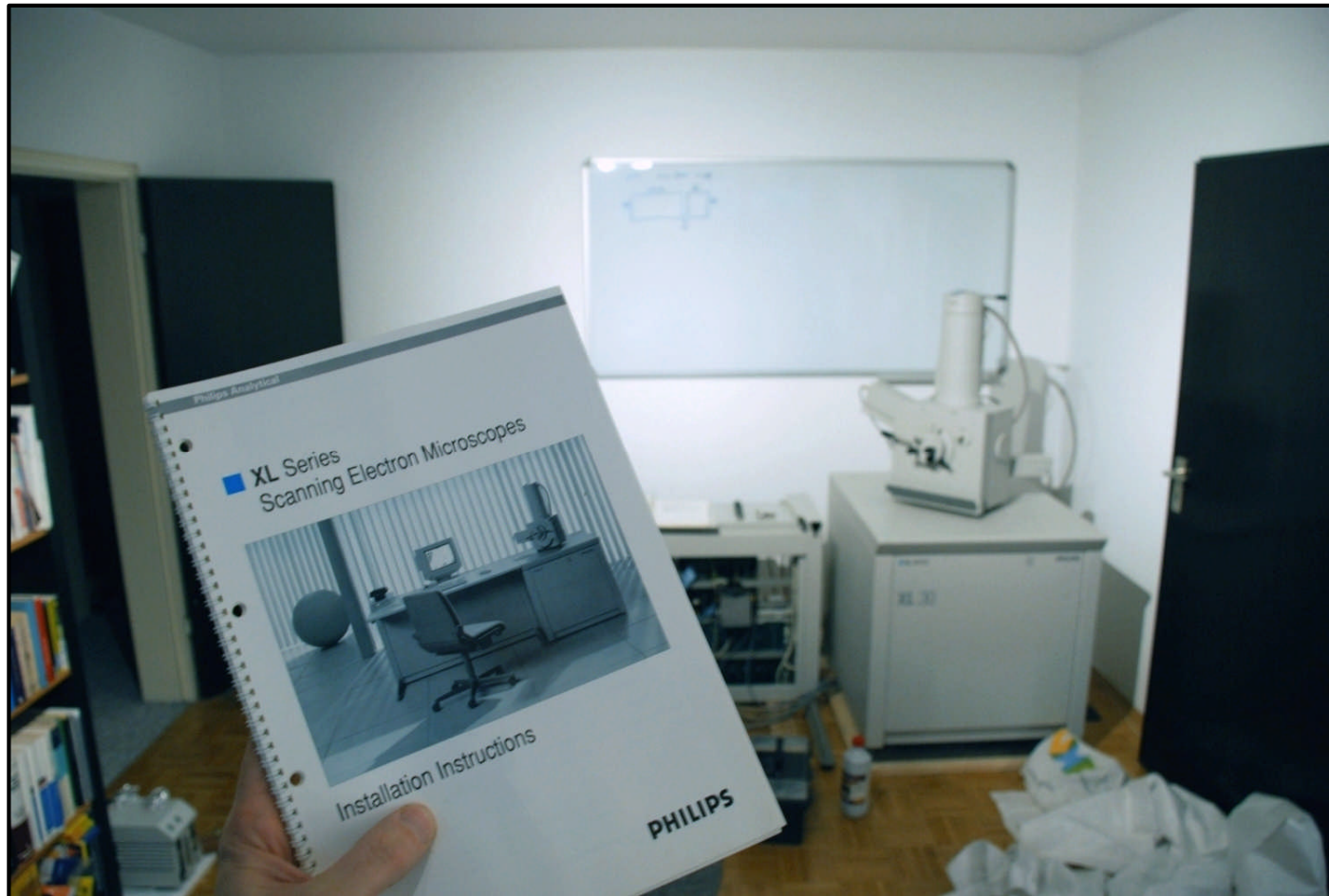
„Who has an Electron Microscope at home ?“ We do, and you can...



1. Reserve a place in your living room...

Pictures: Private Archive M.Janke, P.Laackmann

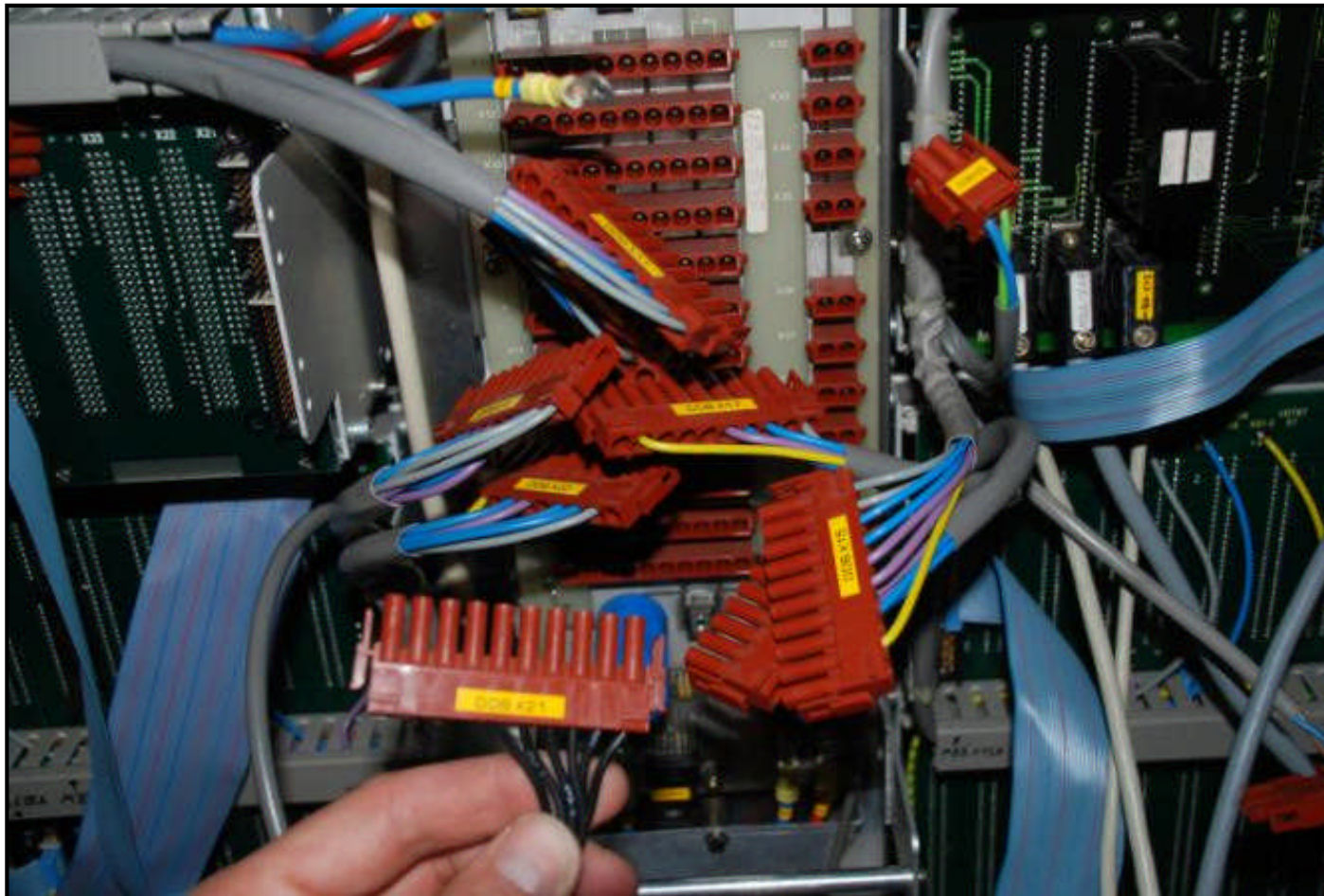
„Who has an Electron Microscope at home ?“
We do, and you can...



2. Read the manual !

Pictures: Private Archive M.Janke, P.Laackmann

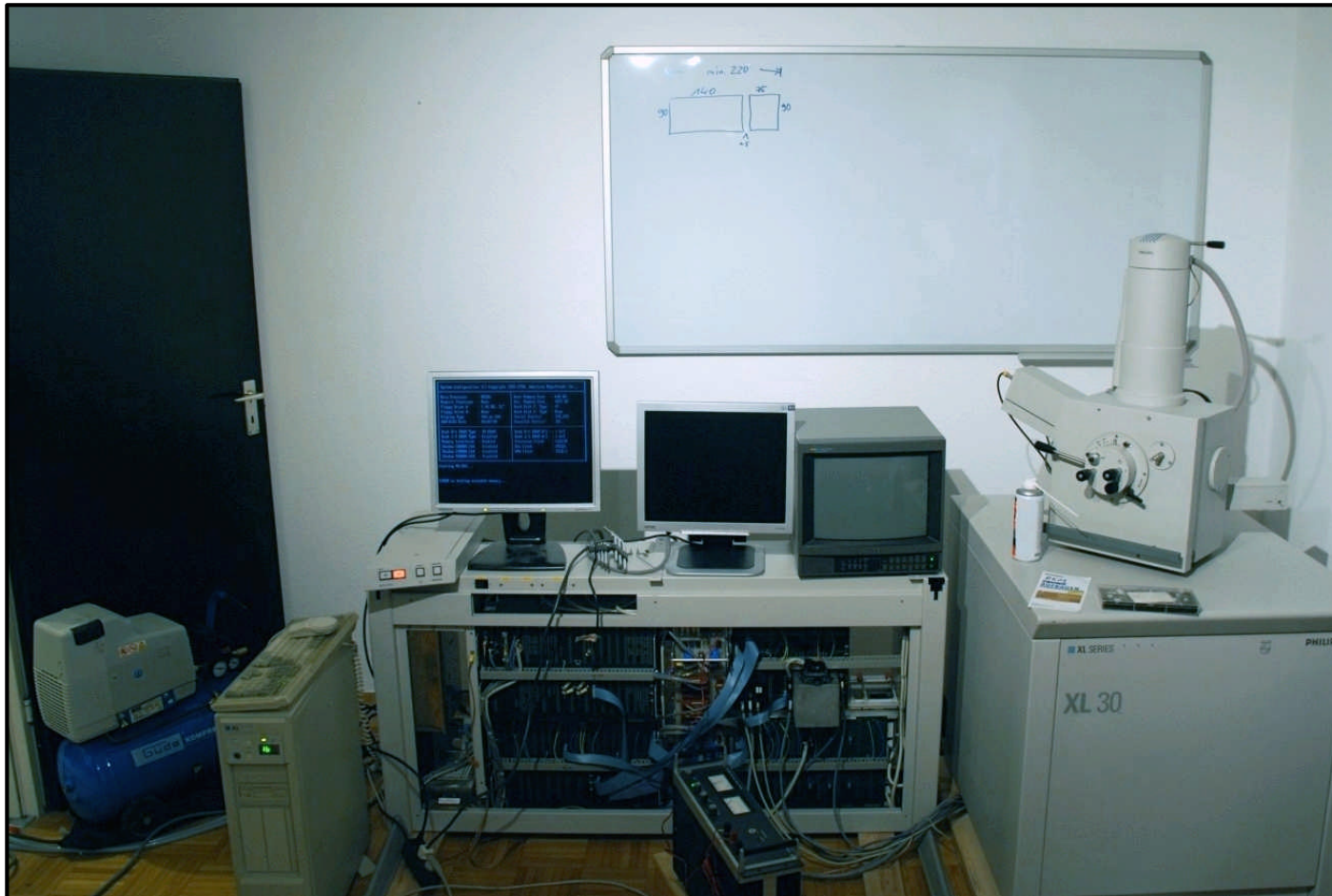
„Who has an Electron Microscope at home ?“
We do, and you can...



3. Connect several dozens of cables, compressed air and water

Pictures: Private Archive M.Janke, P.Laackmann

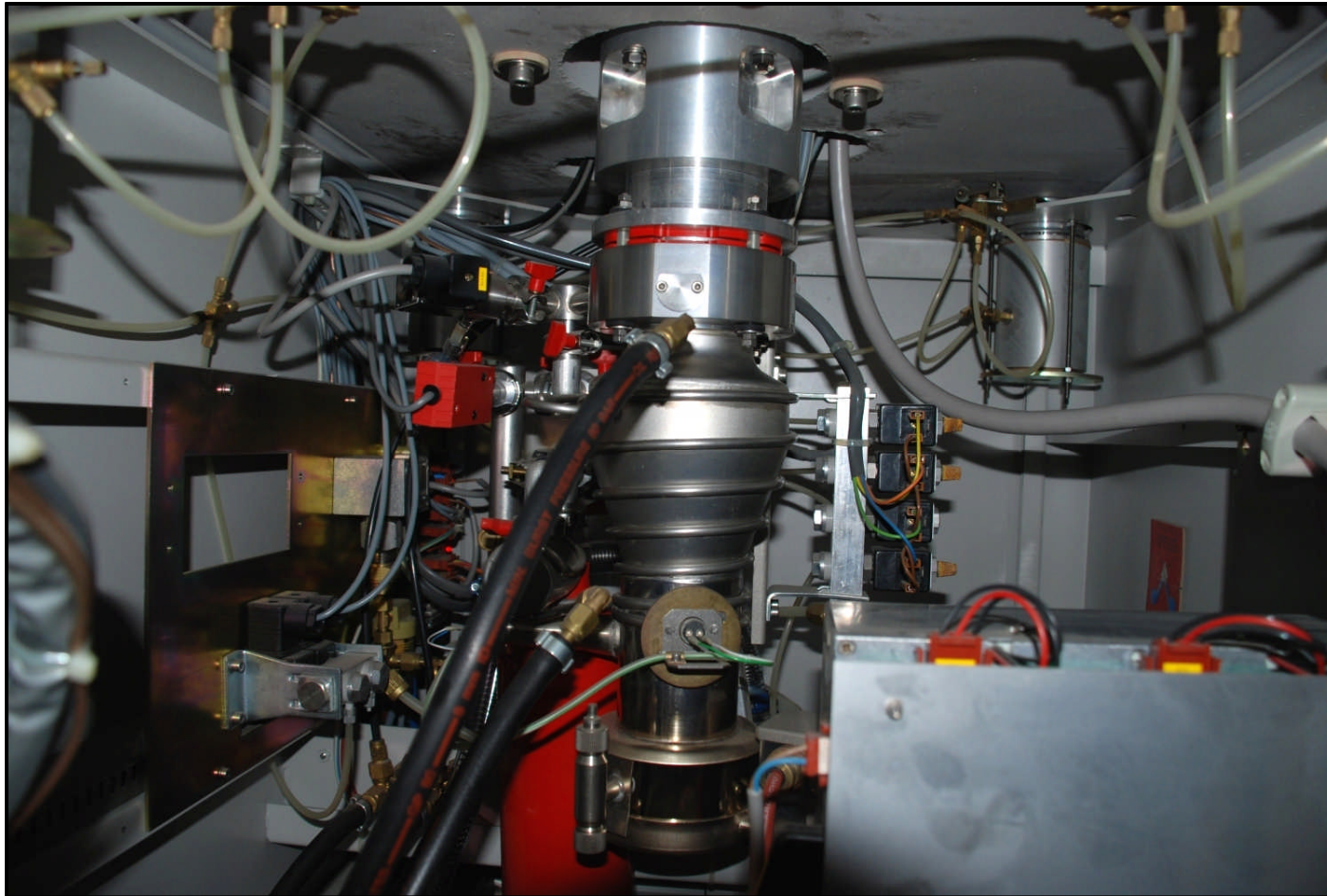
„Who has an Electron Microscope at home ?“
We do, and you can...



4. Prepare for first test and debugging

Pictures: Private Archive M.Janke, P.Laackmann

„Who has an Electron Microscope at home ?“
We do, and you can...



5. Check vacuum system (oil-diffusion pump is great for amateurs !)

Pictures: Private Archive M.Janke, P.Laackmann

„Who has an Electron Microscope at home ?“
We do, and you can...



6. Use system in original configuration, or...

Pictures: Private Archive M.Janke, P.Laackmann

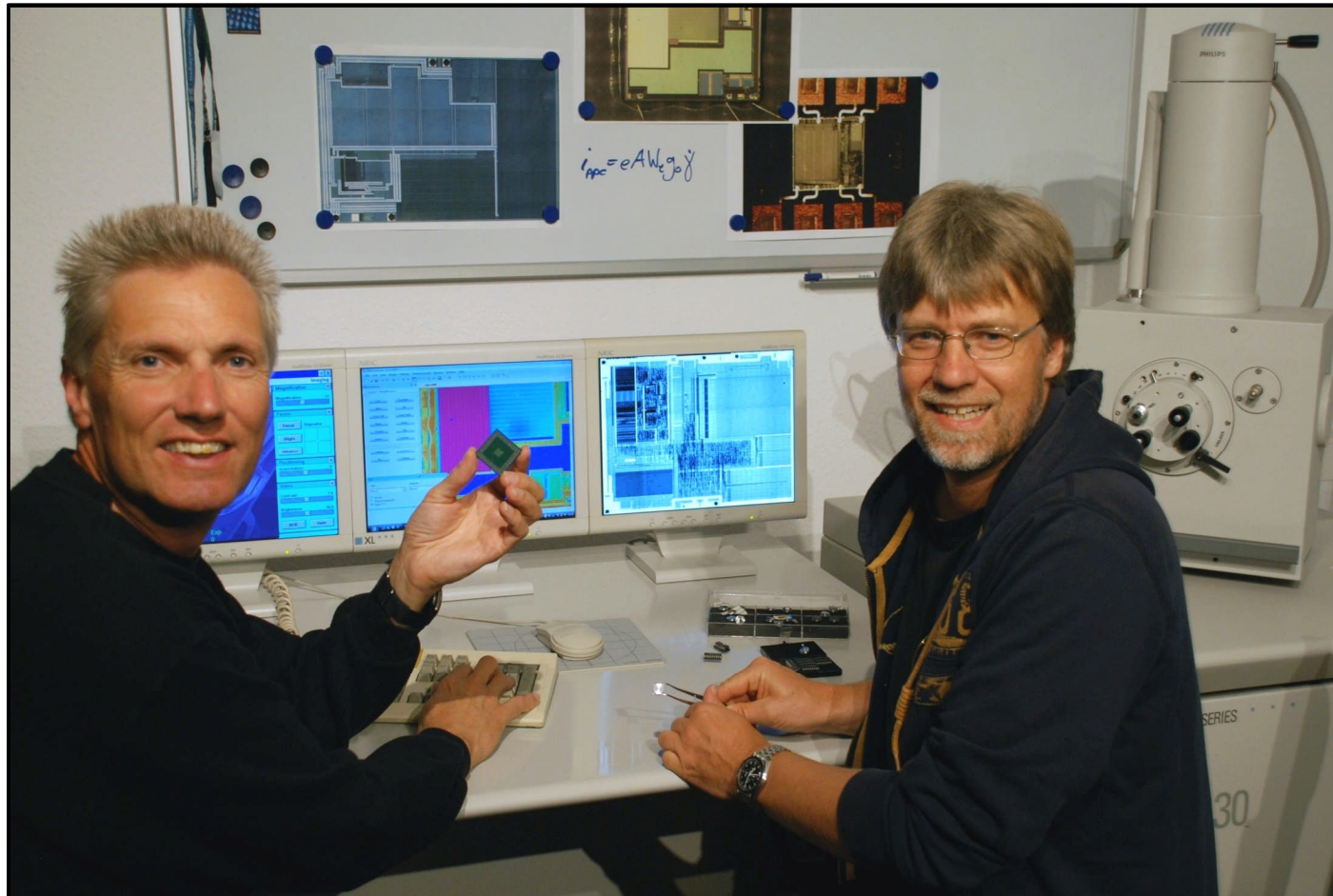
„Who has an Electron Microscope at home ?“
We do, and you can...



7. Modernize a little bit, if you want.

Pictures: Private Archive M.Janke, P.Laackmann

Have Fun Researching !



Pictures: Private Archive M.Janke, P.Laackmann