Tamper resistance and hardware security

Dr Sergei Skorobogatov

http://www.cl.cam.ac.uk/~sps32 *email: sps32@cam.ac.uk*

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Talk Outline

- Introduction
- Attack awareness
- Tamper protection levels
- Attack methods
  - Non-invasive
  - Invasive
  - Semi-invasive
- Protection against attacks
- Conclusions
- Slides
  - http://www.cl.cam.ac.uk/~sps32/PartII_241108.pdf
- Literature:
  - http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.pdf

Introduction

- Protection of systems and devices against physical attacks
  - Protecting secrets from being stolen
  - Preventing unauthorised access
  - Protecting intellectual property from piracy
  - Preventing fraud
- Examples
  - Locks and sensors to prevent physical access
  - Smartcards to hold valuable data and secret keys
  - Electronic keys, access cards and hardware dongles for authentication
  - Service cards for restricted access
  - Cryptoprocessors and crypto-modules for encryption
  - Other examples

Introduction

- Access protection level
  - Lid switch sensor
  - Environment sensors
  - Tamper detection and tamper evidence
- Software level protection
  - Password protection
  - Encryption
  - Protocols
- Hardware level protection
  - Electronics (PCB, sensors)
  - Microelectronics (silicon implementation)

Introduction

- Technical progress pushed secure semiconductor chips towards ubiquity
  - Car industry (anti-theft protection, spare parts identification)
  - Accessory control (mobile phone batteries, printer toner cartridges, memory modules)
  - Access control (RF tags, cards, tokens and dongles)
  - Home entertainment and consumer electronics
  - Intellectual property protection (software copy protection, protection of algorithms, protection from cloning)
- Challenges
  - Design the secure system (hardware security engineering task)
  - Evaluate the threat (how expensive is to break the protection?)
  - Reduce the risk and improve the security

Art of hardware security engineering

- What is the reason to attack your system?
  - Attack scenarios and motivations
- Who is going to attacks your system?
  - Classes of attackers
- What tools would they use for the attacks?
  - Attack categories
  - Attack methods
- How to protect against these attacks?
  - Estimating the threat (understanding motivation, cost and likeness of the attack)
  - Developing adequate protection (locating the right spots)
  - Performing security evaluation

Attack scenarios and motivations

- Cloning and overbuilding
  - Copying for making profit without investment in development
  - Low-cost mass production (subcontractors, outsourcing)
- Access to information
  - Information recovery and extraction
  - Gaining trade secrets (IP piracy)
  - ID theft
- Theft of service
  - Attacks on service providers (satellite TV, electronic meters, access dongles)
- Denial of service
  - Electronic warfare
  - Dishonest competition

Classes of the attackers

D.G.Abraham et al. (IBM), 1991

- Class I (clever outsiders):
  - very intelligent but may have insufficient knowledge of the system
  - have access to only moderately sophisticated equipment
  - often try to take advantage of an existing weakness in the system, rather than try to create one
- Class II (knowledgeable insiders):
  - have substantial specialised technical education and experience
  - have varying degrees of understanding of parts of the system but potential access to most of it
  - often have access to highly sophisticated tools and instruments for analysis
- Class III (funded organisations):
  - able to assemble teams of specialists with related and complementary skills backed by great funding resources
  - capable of in-depth analysis of the system, designing sophisticated attacks, and using the most advanced analysis tools
  - may use Class II adversaries as part of the attack team

Attack categories

- Eavesdropping
  - techniques that allows the attacker to monitor the analog characteristics of supply and interface connections and any electromagnetic radiation
- Software attacks
  - use the normal communication interface and exploit security vulnerabilities found in the protocols, cryptographic algorithms, or their implementation
- Fault generation
  - use abnormal environmental conditions to generate malfunctions in the system that provide additional access
- Microprobing
  - can be used to access the chip surface directly, so we can observe, manipulate, and interfere with the device
- Reverse engineering
  - used to understand the inner structure of the device and learn or emulate its functionality; requires the use of the same technology available to semiconductor manufacturers and gives similar capabilities to the attacker

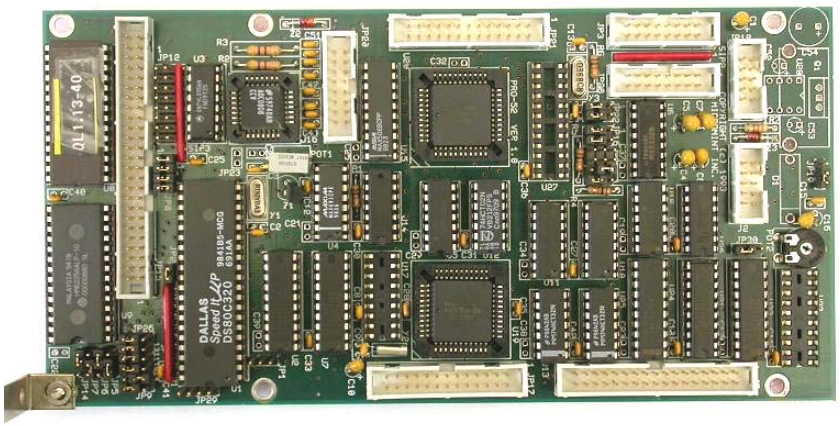
Attack methods

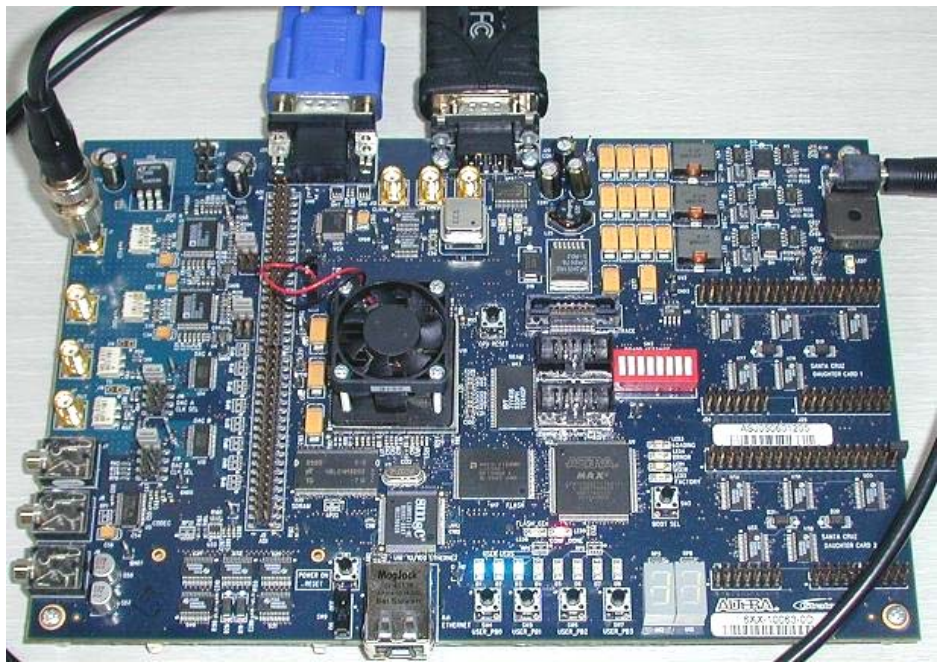
- Non-invasive attacks
  - Observe or manipulate with the device without physical harm to it
  - Require only moderately sophisticated equipment and knowledge to implement
- Invasive attacks
  - Almost unlimited capabilities to extract information from chips and understand their functionality
  - Normally require expensive equipment, knowledgeable attackers and time
- Semi-invasive attacks
  - Semiconductor chip is depackaged but the internal structure of it remains intact
  - Fill the gap between non-invasive and invasive types, being both inexpensive and easily repeatable

Tamper protection levels

D.G.Abraham et al. (IBM), 1991

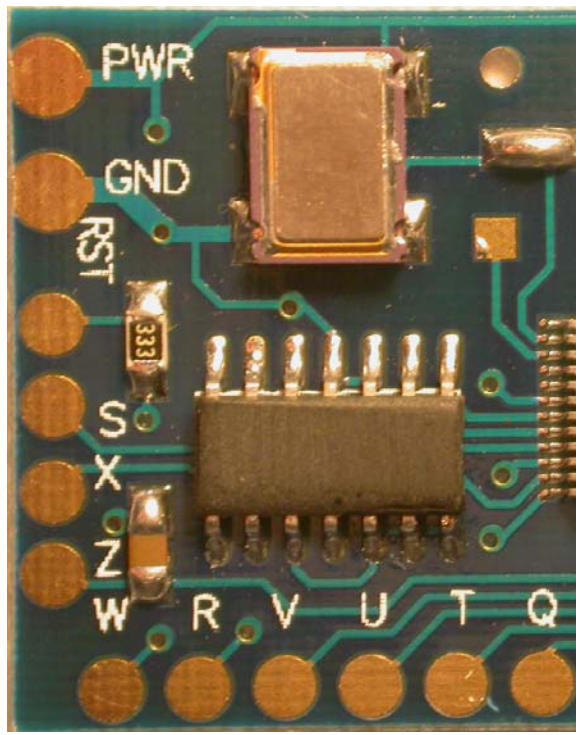
- Level ZERO (no special protection)
  - Microcontroller or FPGA with external ROM
  - No special security features are used. All parts have free access and can be easily investigated. Low cost and less than an hour to attack





Tamper protection levels

- Level LOW
  - Microcontrollers with proprietary read algorithm, remarked ICs
  - Some security features are used but they can be relatively easy defeated with minimum tools required. Low cost, but takes some time to learn and attack



Tamper protection levels

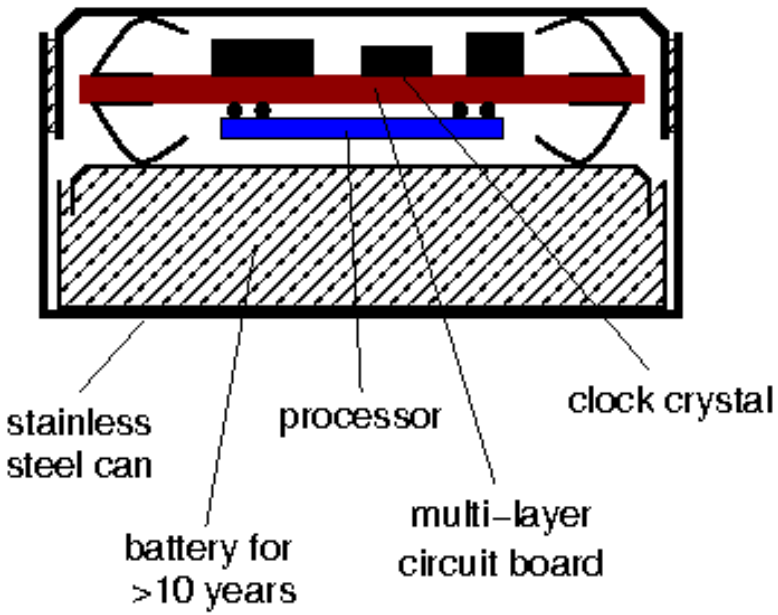
- Level MODL
  - Microcontrollers with security protection, low-cost hardware dongles
  - Protection against many low-cost attacks. Relatively inexpensive tools are required, but some knowledge is necessary. Moderate cost and days to weeks to attack

Tamper protection levels

- Level MOD
  - Smartcards, high-security microcontrollers, ASICs, CPLDs, hardware dongles, i-Buttons
  - Special tools and equipment are required for successful attack as well as some special skills and knowledge. High cost and weeks to months to attack

Tamper protection levels

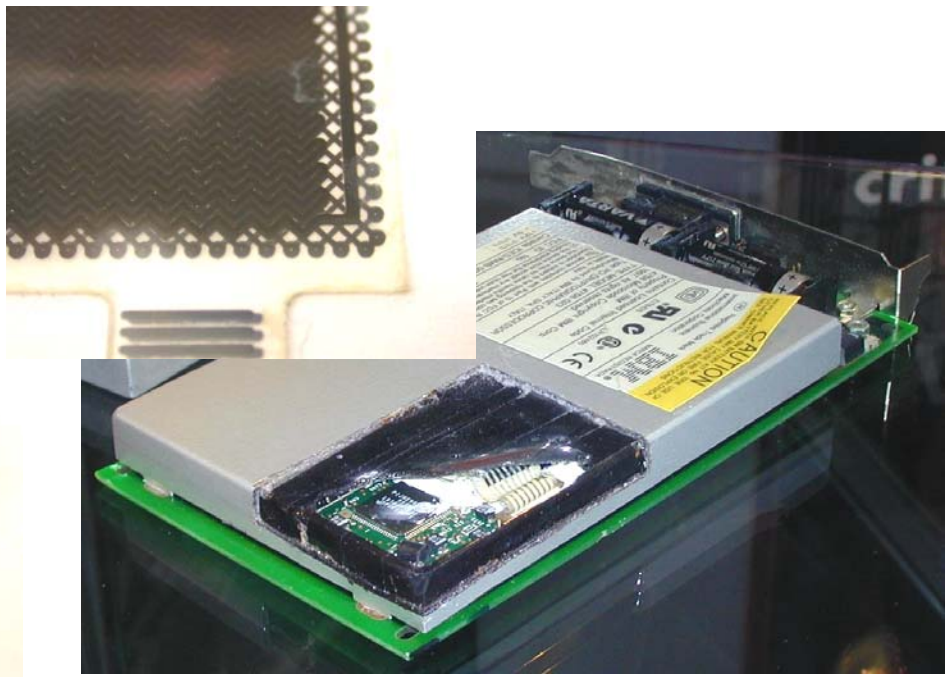
- Level MODH
  - Secure i-Buttons, secure FPGAs, high-end smartcards and ASICs
  - Special attention is paid to design of the security protection. Equipment is available but is expensive to buy and operate. Very high cost and months to attack



Picture courtesy of Dr Markus Kuhn

Tamper protection levels

- Level HIGH
  - Military and bank equipment
  - All known attacks are defeated. Some research by a team of specialists is necessary to find a new attack. Extremely high cost and years to attack



Picture courtesy of Dr Markus Kuhn

Tamper protection levels

- Division to levels from ZERO to HIGH is relative
  - Some products designed to be very secure might have flaws
  - Some products not designed to be secure might still end up being very difficult to attack
  - Technological progress opens doors to less expensive attacks, thus reducing the protection level of some products
- Proper security evaluation must be carried out to estimate whether products comply with all the requirements
  - Design overview for any possible security flaws
  - Test against known attacks

Non-invasive attacks

- Non-penetrative to the attacked device
  - Normally do not leave tamper evidence of the attack
- Tools
  - Digital multimeter
  - IC soldering/desoldering station
  - Universal programmer and IC tester
  - Oscilloscope
  - Logic analyser
  - Signal generator
  - Programmable power supplies
  - PC with data acquisition board or FPGA boards
  - PCB prototyping boards

Non-invasive attacks

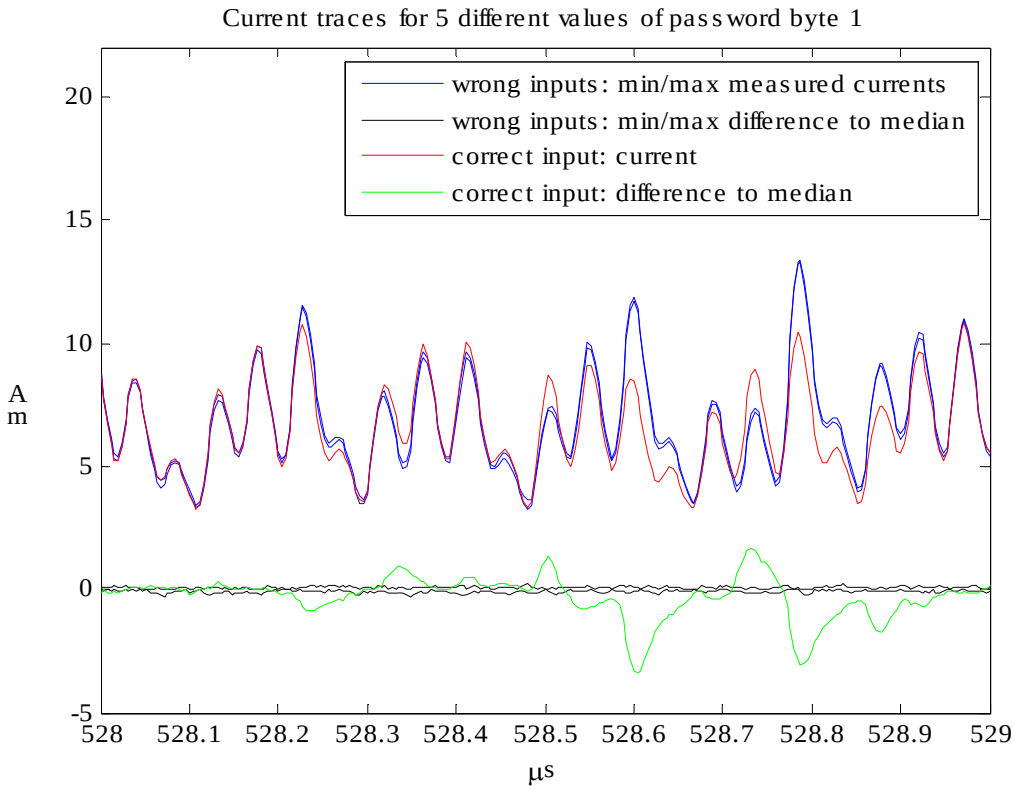
- Timing attacks
  - Different computation time for different conditions
    - Incorrect password verification
      - Termination on incorrect byte
      - Different computation length for incorrect bytes
    - Incorrect implementation of encryption algorithms
      - Performance optimisation (conditional branches)
      - Cache memory usage
      - Non-fixed time processor instructions (multiplication, division)
- Brute force attacks
  - Searching for keys and passwords
    - Inefficient selection of keys and passwords
  - Recovering design from CPLDs, FPGAs and ASICs
  - Eavesdropping on communication to find hidden functions

Non-invasive attacks

- Power analysis: Measuring power consumption in time (voltage drop over a 10Ω resistor)
  - Very simple set of equipment – a PC with an oscilloscope, but some knowledge in electrical engineering and digital signal processing is required
  - Very effective against many cryptographic algorithms and password verification schemes
  - To find a difference in an instruction flow, a single trace acquired with a high resolution is enough
  - When a difference in a single bit of data is required, average over hundreds or thousands of power traces is necessary

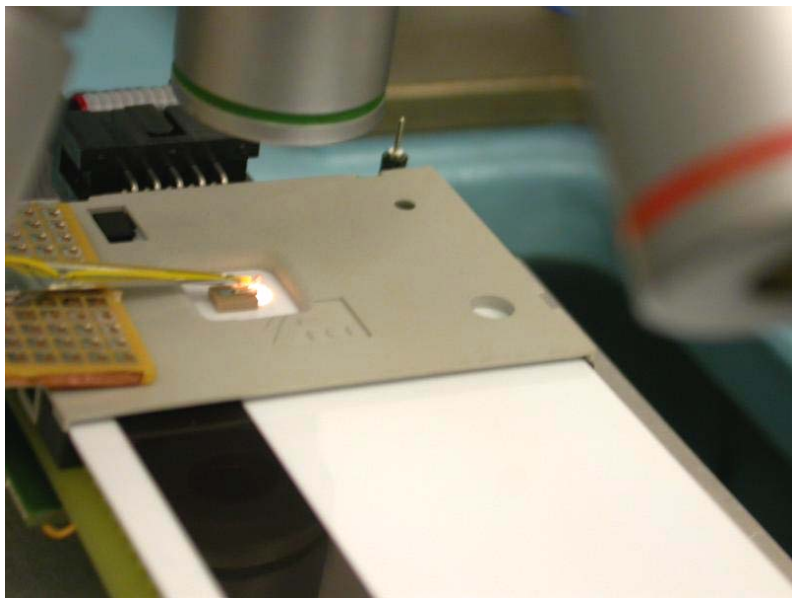
Non-invasive attacks

- Power analysis
  - 8-byte password check in Freescale MC908AZ60A microcontroller
  - 1 byte at a time, 1 of 256 attempts leads to distinctive power trace
  - Full password recovery in 2048 attempts (less than 10 minutes)



Non-invasive attacks

- Electro-magnetic analysis (EMA)
  - Similar to power analysis, but instead of a resistor, a small magnetic coil is used
  - By placing the coil close to the part of circuit that performs the critical computations, better signals can be observed
  - Our experiments showed that very little advantage over conventional power analysis can be achieved



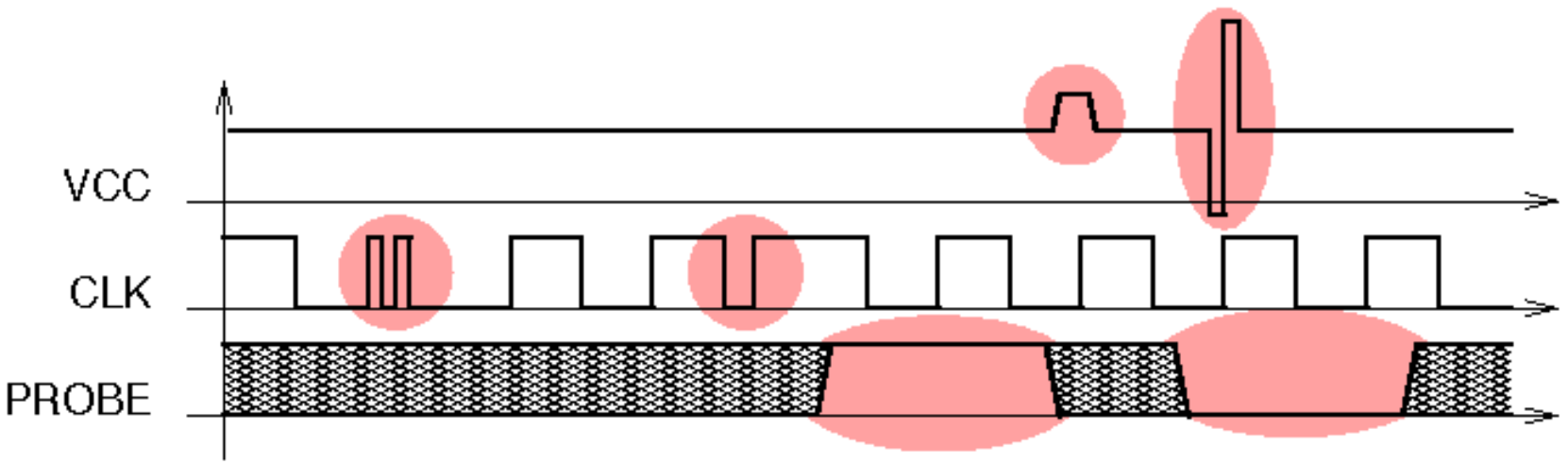
Non-invasive attacks

- Glitch attacks
  - Clock glitches
  - Power glitches
- Security fuse verification in the Mask ROM bootloader of the Motorola MC68HC05B6 microcontroller
  - Double frequency clock glitching
  - Low-voltage power glitching (1.8 – 2.2 V vs standard V_{DD} = 5 V)

```
        LDA     #01h
        AND     $0100           ;the contents of the EEPROM byte is checked
loop:   BEQ     loop            ;endless loop if bit 0 is zero
        BRCLR   4, $0003, cont  ;test mode of operation
        JMP     $0000           ;direct jump to the preset address
cont:   … … …
```

Non-invasive attacks

- Glitch attacks
  - Change single instructions or data
    - Links between gates form RC delay elements. Maximum RC sum of any signal path determines maximum CLK frequency
    - Transistors compare internal signals with a part of V_{CC} (usually ½), which allows V_{CC} glitches



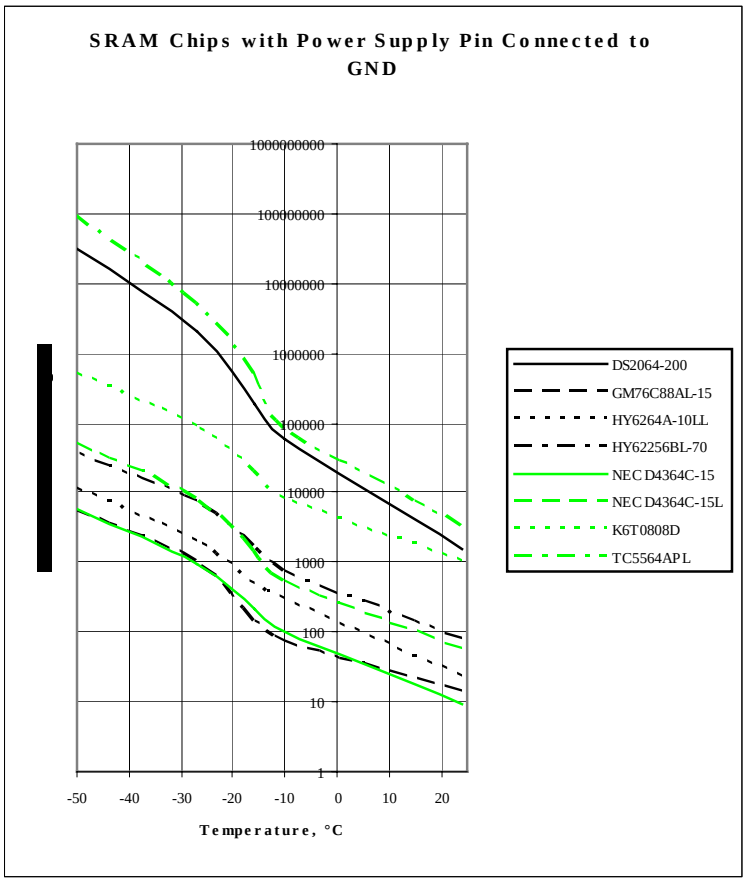
Picture courtesy of Dr Markus Kuhn

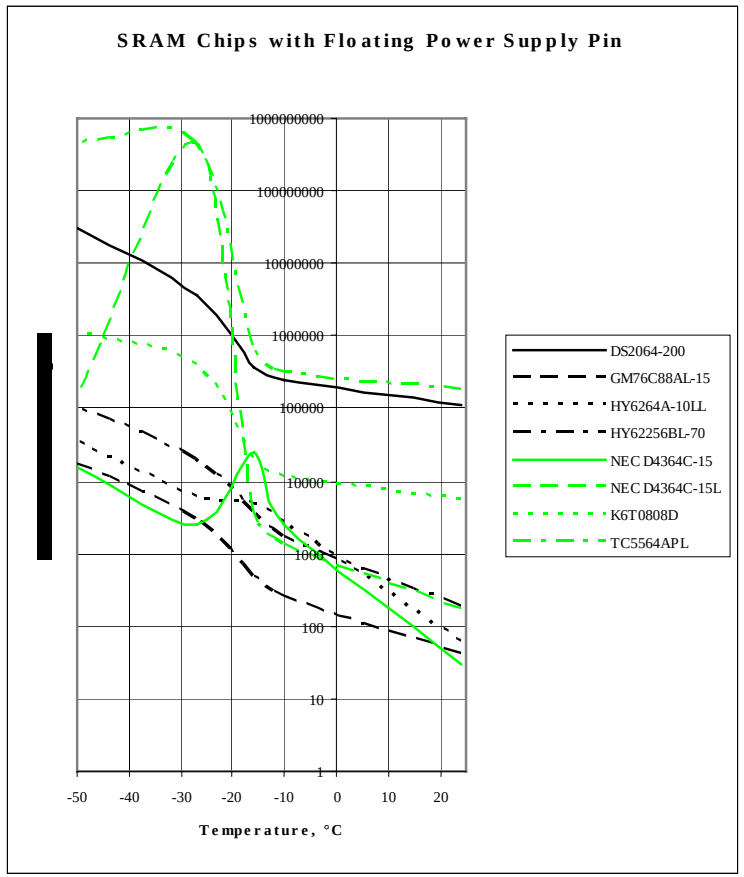
Non-invasive attacks

- Data remanence in SRAM
  - Residual representation of data after erasure
    - First discovered in magnetic media
  - Low temperature data remanence
    - Dangerous to tamper resistant devices which store keys and secret data in a battery backed-up SRAM
  - Long period data storage
    - Ion migration and electromigration effects
    - Dangerous to secure devices which store keys at the same memory location for years

Non-invasive attacks

- Low temperature data remanence in SRAM
  - Eight SRAM samples were tested at different temperatures
  - Grounding the power supply pin reduces the retention time



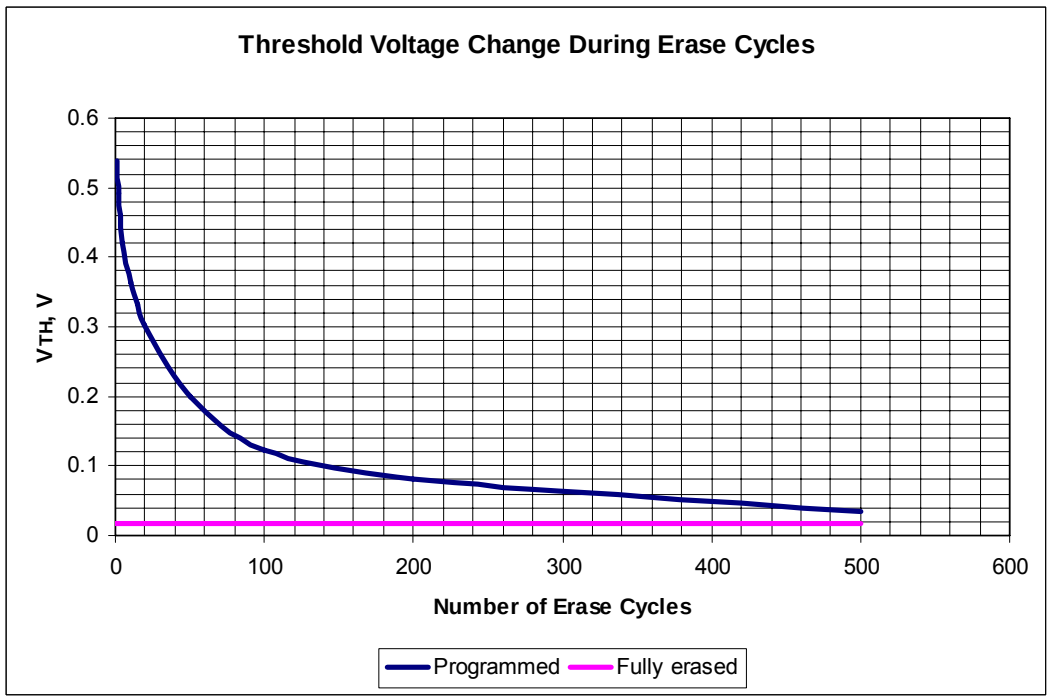


Non-invasive attacks

- Data remanence in non-volatile memories
  - EPROM, EEPROM and Flash
    - Widely used in microcontrollers and smartcards
    - Floating-gate transistors, 10^3 – 10^5 e^- , ΔV_{TH} ~ 3.5 V
  - Levels of remanence threat
    - File system (erasing a file → undelete)
    - File backup (software features)
    - Smart memory (hardware buffers)
    - Memory cell
  - Possible outcomes
    - Circumvention of microcontroller security
    - Information leakage through shared EEPROM areas between different applications in smartcards

Non-invasive attacks

- Data remanence in EEPROM and Flash
  - $V_{TH} = V_{ref} = K\,V_{DD} - V_W$, $K = 0.5$, $V_W = 0.7$ V
  - Memory bulk erase cycles
    - Flash memory, after 100 erase cycles: $\Delta V_{TH} = 100$ mV
    - EEPROM memory, after 10 erase cycles: $\Delta V_{TH} = 1$ mV

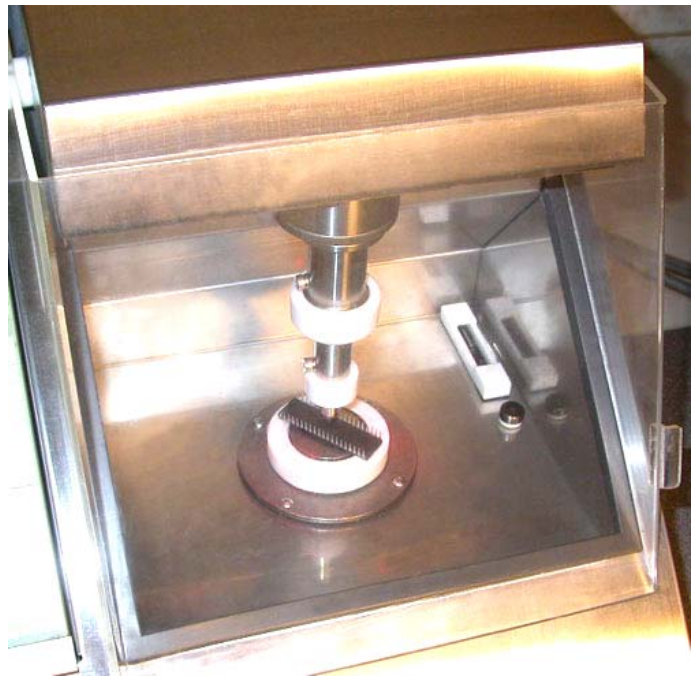


Invasive attacks

- Penetrative attacks
  - Leave tamper evidence of the attack or even destroy the device
- Tools
  - IC soldering/desoldering station
  - Simple chemistry lab
  - Wire bonding machine
  - PCB prototyping boards
  - Signal generator, logic analyser and oscilloscope or PC with data acquisition board
  - Laser cutting system
  - Microprobing station
  - High-resolution optical microscope
  - Scanning electron microscope (SEM)
  - Focused Ion Beam (FIB) workstation

Invasive attacks

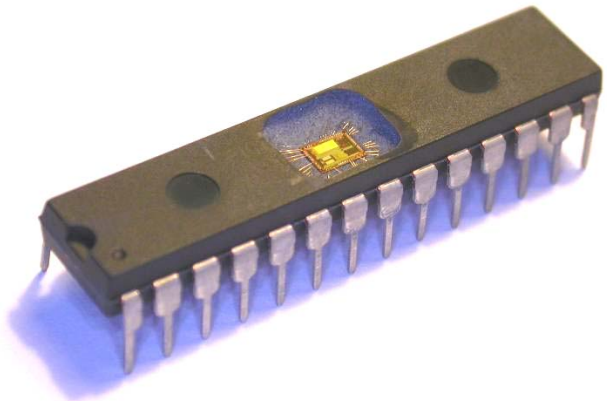
- Sample preparation
  - Decapsulation
    - Manual: using fuming nitric acid (HNO_3) and Acetone, 60 °C
    - Automatic: using hot concentrated HNO_3 and H_2SO_4

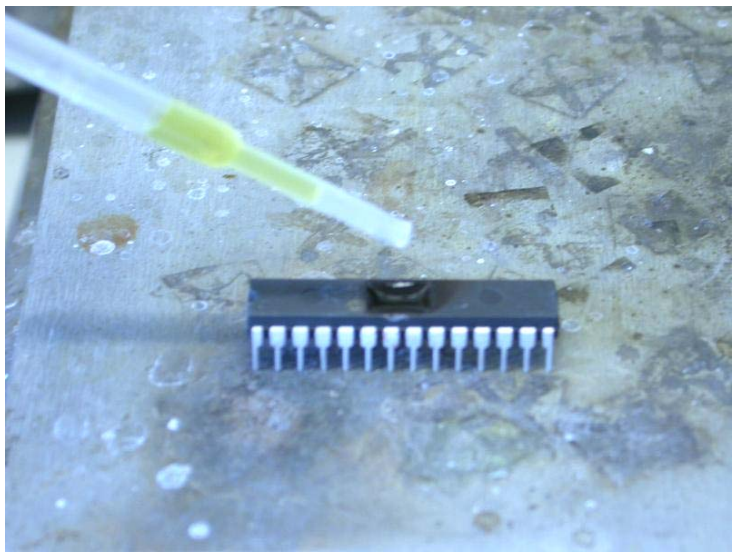


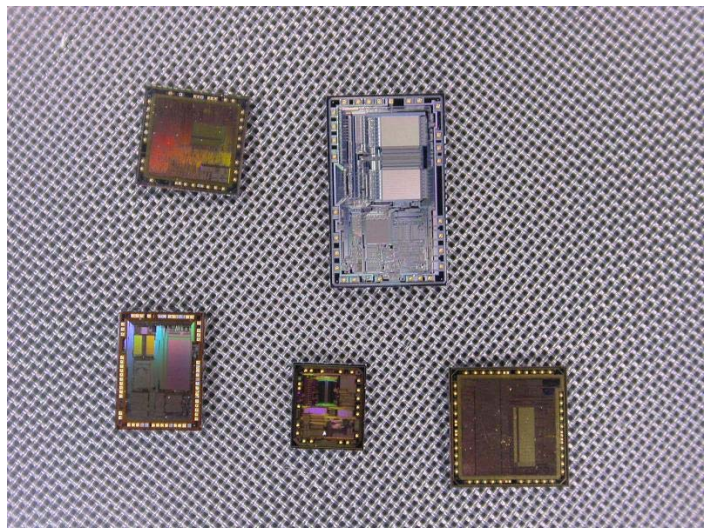
Picture courtesy of Semiresearch Ltd

Invasive attacks

- Sample preparation
  - Decapsulation
    - Front-side and rear-side
    - Partial and full

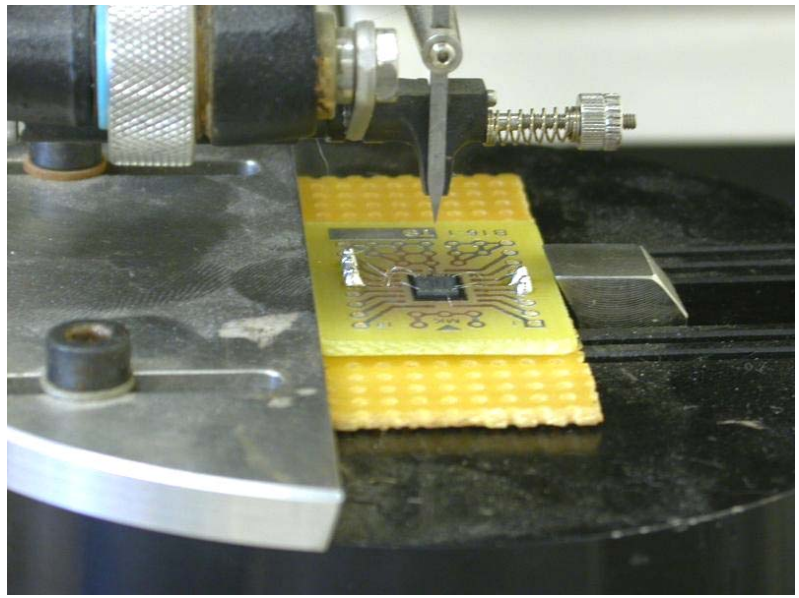






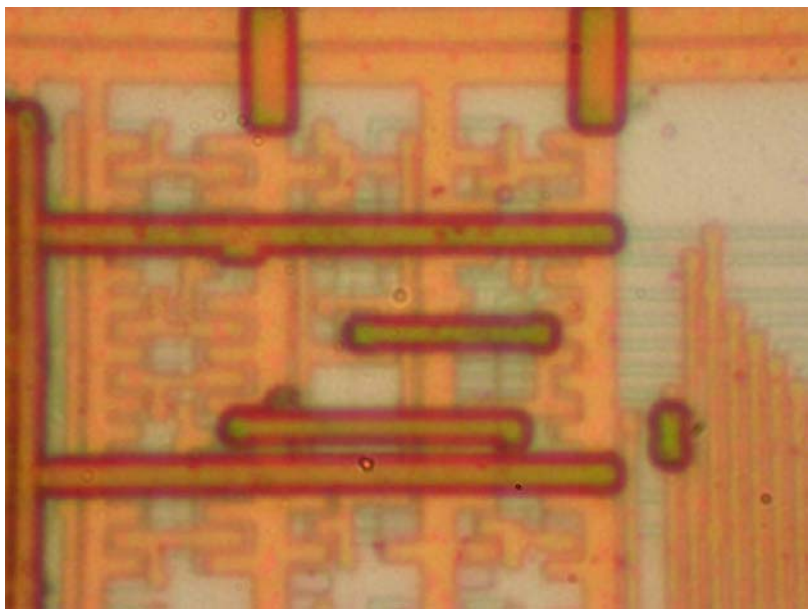
Invasive attacks

- Sample preparation
  - Bonding
    - Wedge wire bonder
    - Gold ball bonder

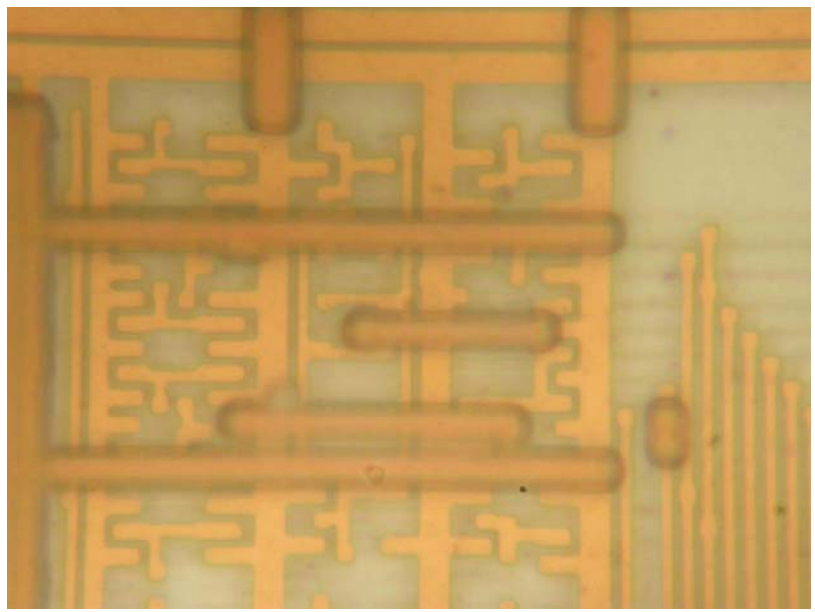


Invasive attacks

- Optical imaging
  - Resolution is limited by optics and wavelength of a light
    - R = 0.61 λ / *NA* = 0.61 λ / *n* sin(μ)
      - Reducing wavelength of the light (using UV sources)
      - Increasing refraction index of the medium (using immersion oil: *n* = 1.5)
      - Increasing the angular aperture (dry objectives have *NA* = 0.95)



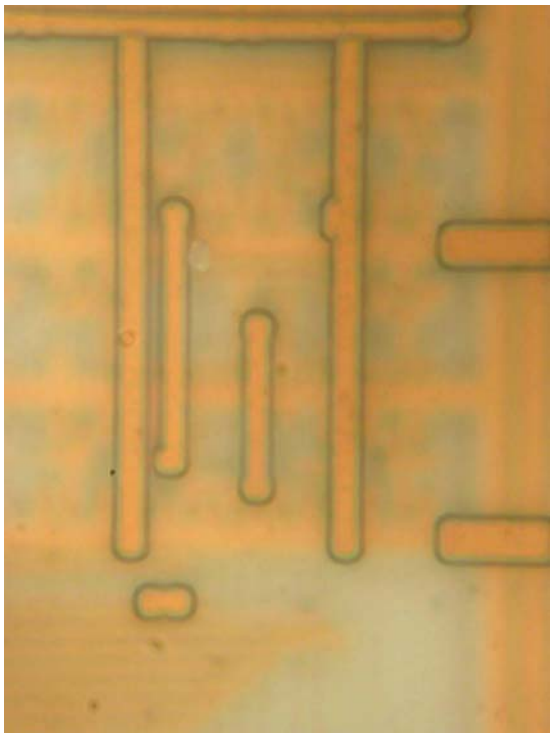
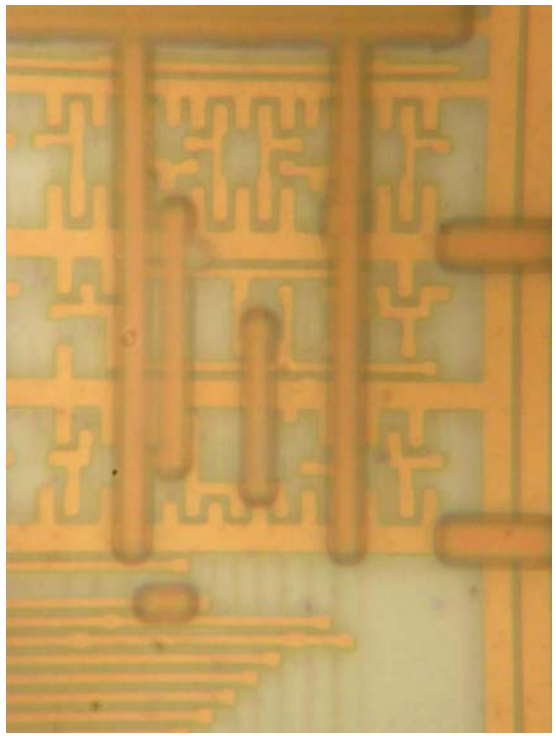
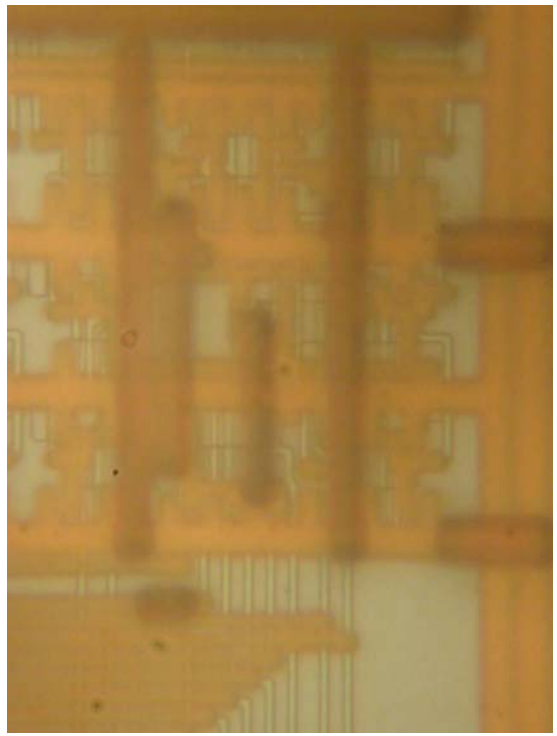
Bausch&Lomb MicroZoom, 50×2×, NA = 0.45



Leitz Ergolux AMC, 100×, NA = 0.9

Invasive attacks

- Optical imaging
  - Image quality depends on microscope optics
    - Depth of focus
    - Geometric distortions (pose problem for later postprocessing)

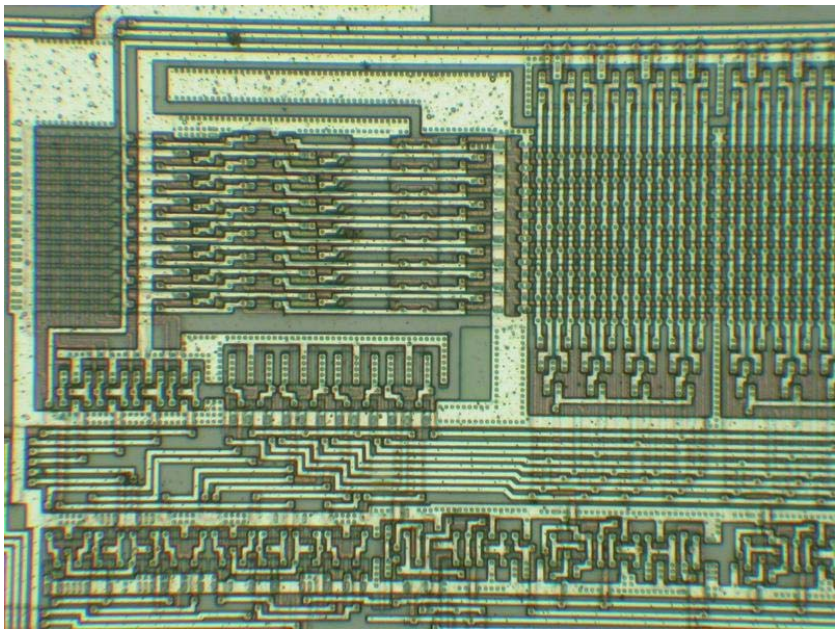




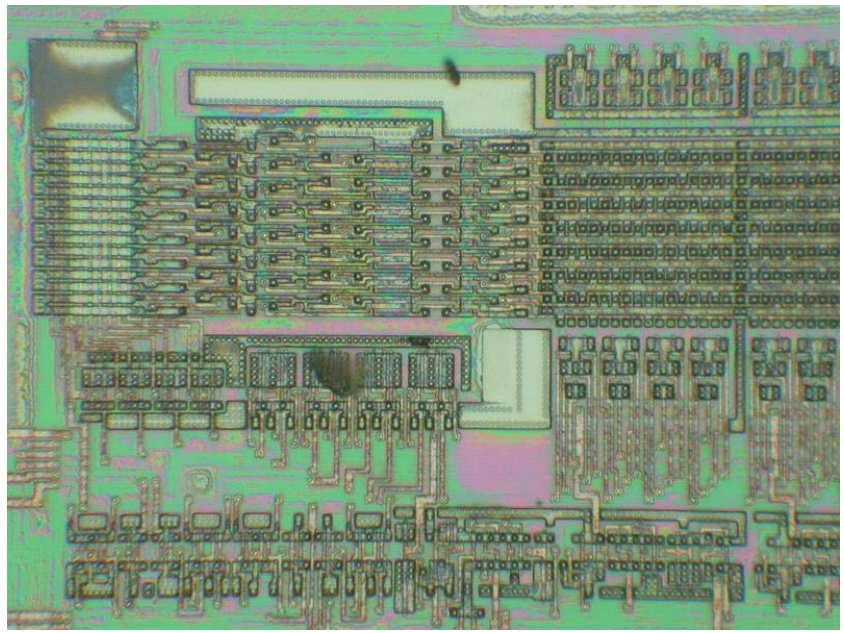
Invasive attacks

- Deprocessing
  - Removing passivation layer, exposing the top metal layer for microprobing attacks
  - Decomposition of a chip for reverse engineering
  - Mask ROM extraction
- Methods
  - Wet chemical etching (KOH solutions, HCl, H_2O_2)
    - Isotropic – uniformity in all directions
    - Uneven etching and undercuts (metal wires lift off the surface)
  - Plasma etching or dry etching (CF_4, C_2F_6, SF_6 or CCl_4 gases)
    - Perpendicular to the surface
    - Speed varies for different materials
  - Chemical-mechanical polishing (abrasives like Al_20_3 or diamond)
    - Good planarity and depth control, suitable for modern technologies
    - Difficult to maintain planarity of the surface, special tools required

Invasive attacks

- Removing top metal layer using wet chemical etching
  - Good uniformity over the surface
  - Works reliably only for chips fabricated with 0.8 μm or larger technology (without polishing layers)

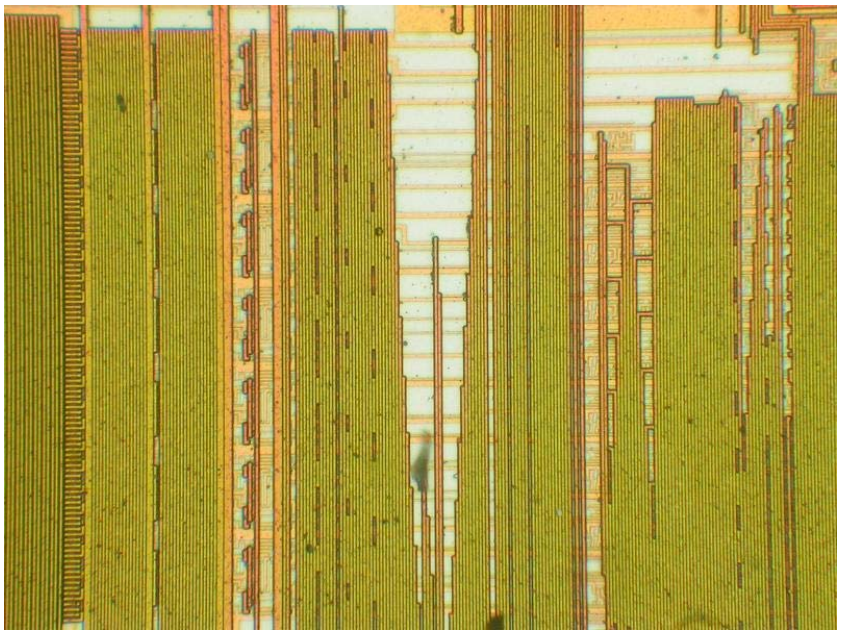


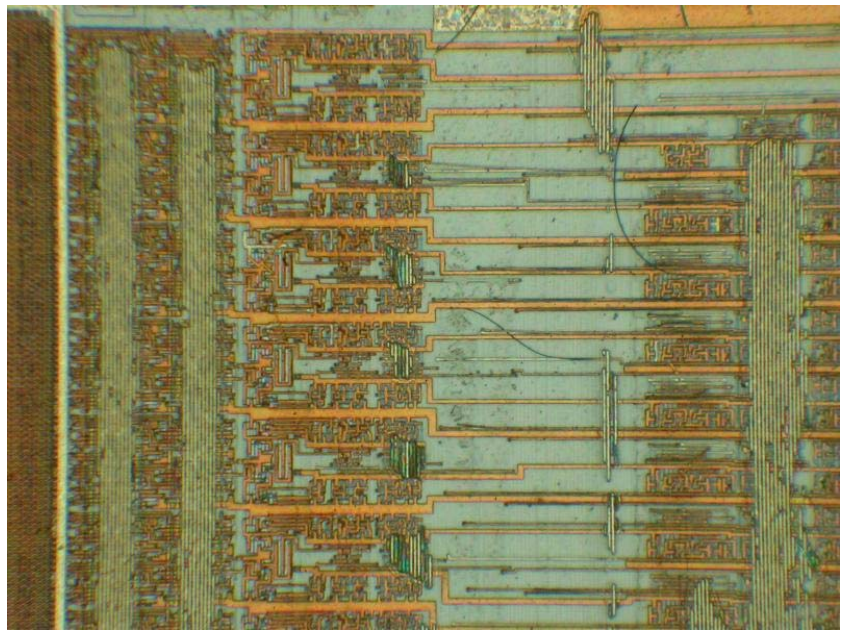


Motorola MC68HC705C9A microcontroller

Invasive attacks

- Removing top metal layer using wet chemical etching
  - Unsuitable for chip fabricated with 0.5 μm or smaller technology (with chemical-mechanical polishing) because of undercuts, under- and over-etching

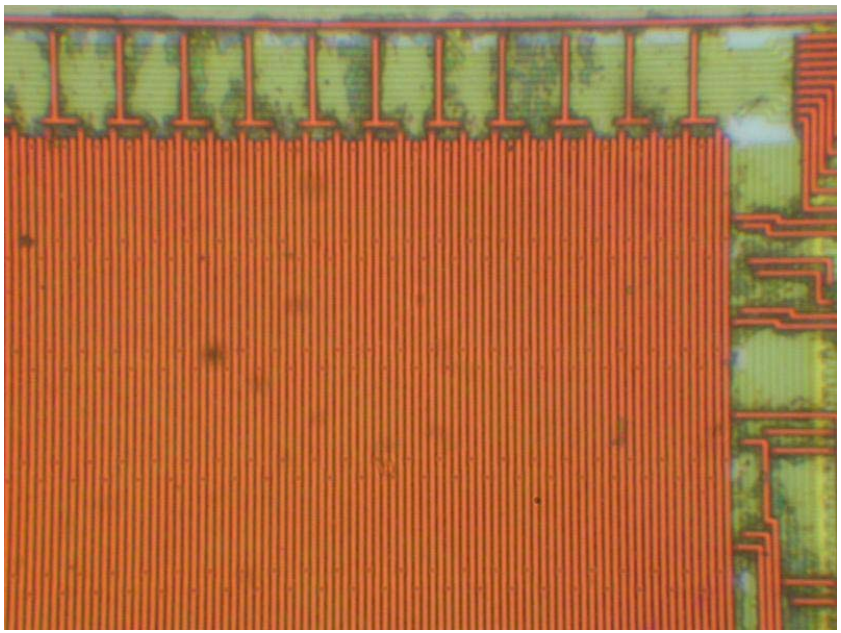


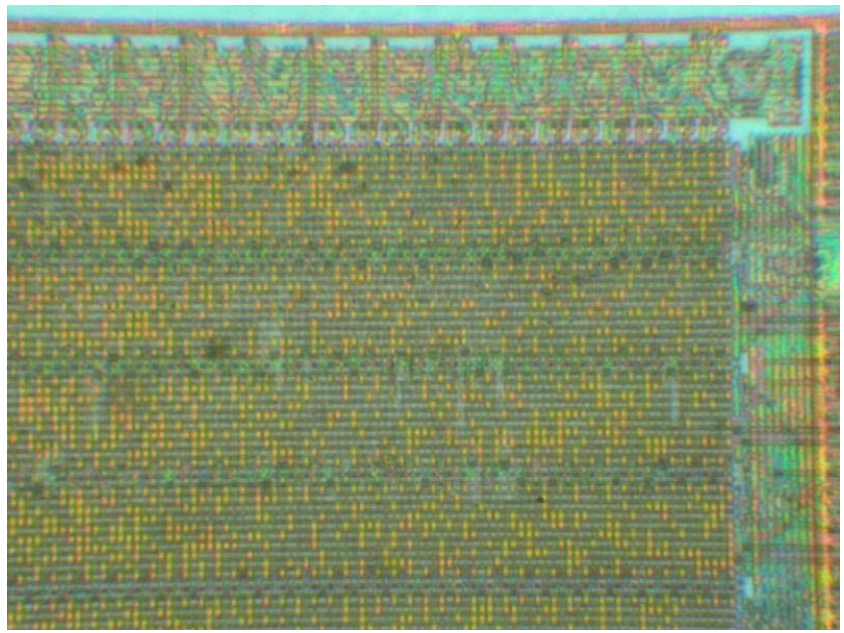


Microchip PIC16F76 microcontroller

Invasive attacks

- Memory extraction from Mask ROMs
  - Removing top metal layers for direct optical observation of data in NOR ROMs (bits programmed by presence of transistors)
  - Not suitable for VTROM (ion implanted) used in smartcards



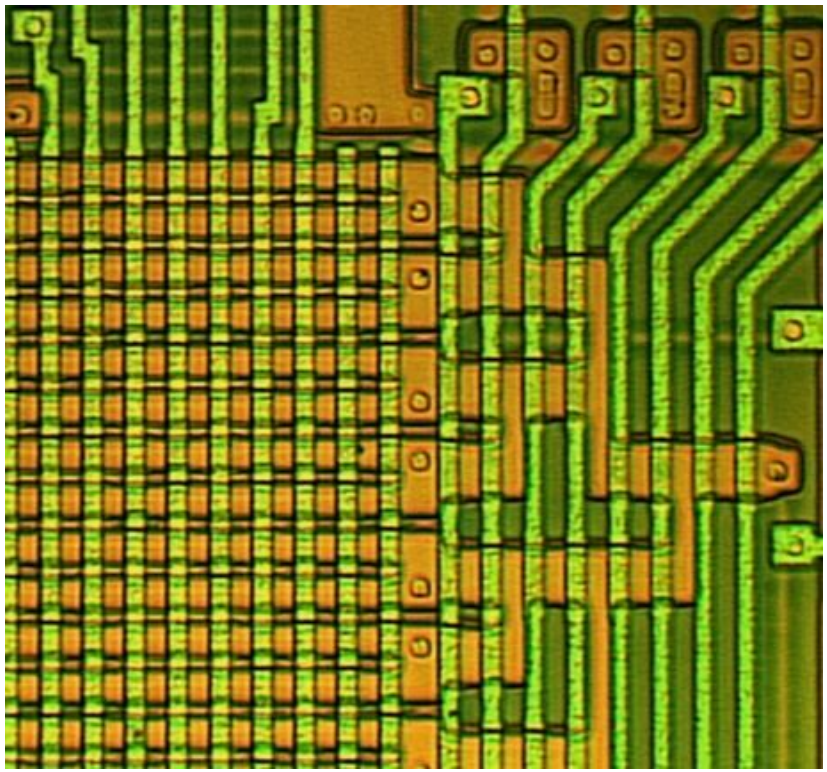


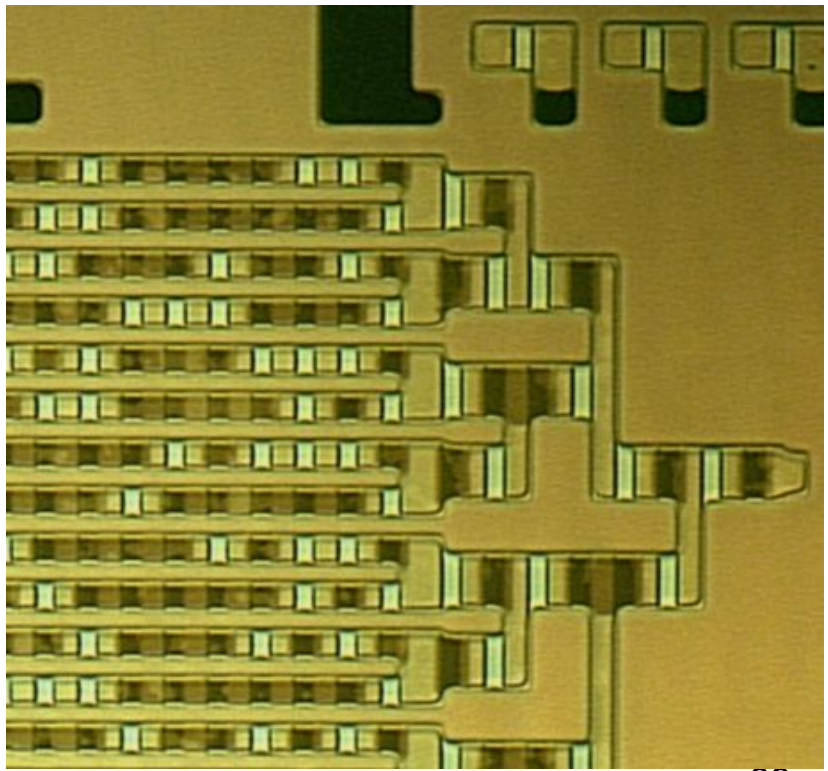
NEC μPD78F9116 microcontroller

Invasive attacks

O. Kömmerling M. Kuhn, 1999

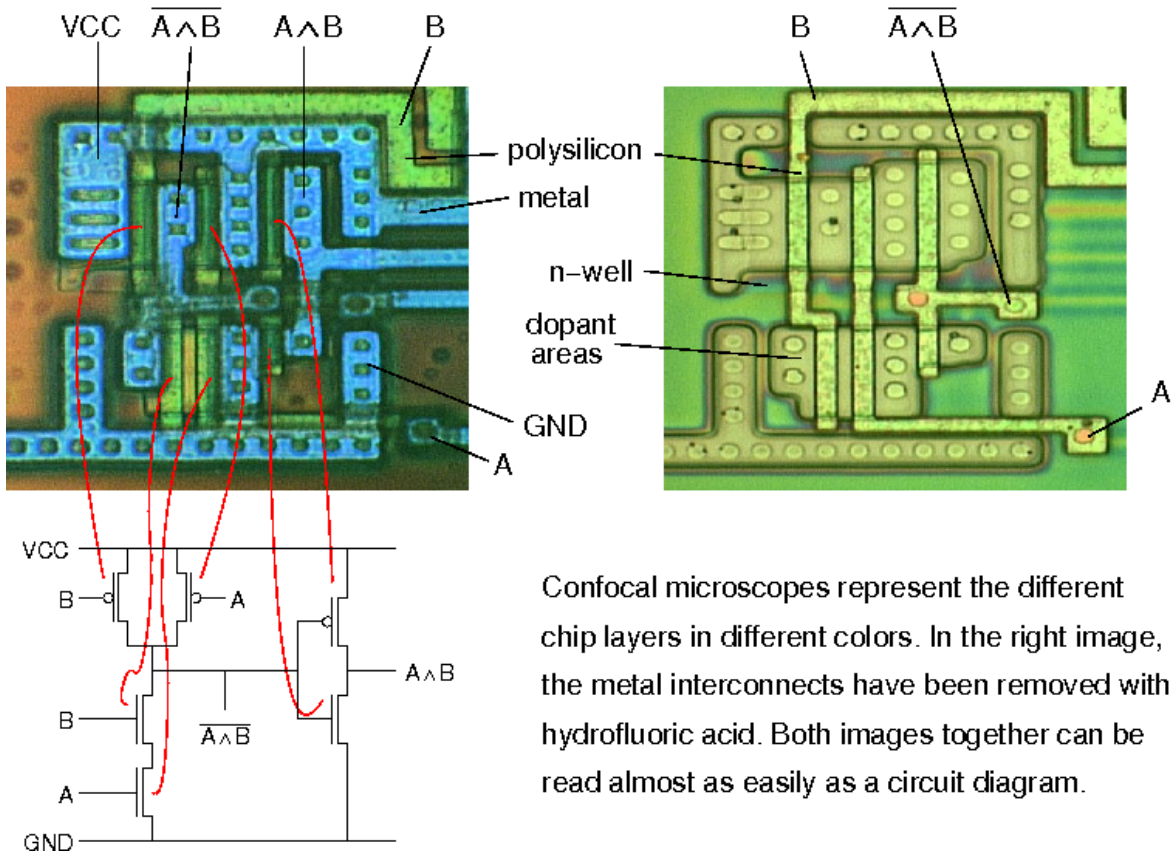
- Memory extraction from Mask ROMs
  - Selective (dash) etchants reacts with doped and non-doped regions at different speeds, exposing the ROM bits





Invasive attacks

- Reverse engineering – understanding the structure of a semiconductor device and its functions
  - Optical – using a confocal microscope (for > 0.5 µm chips)

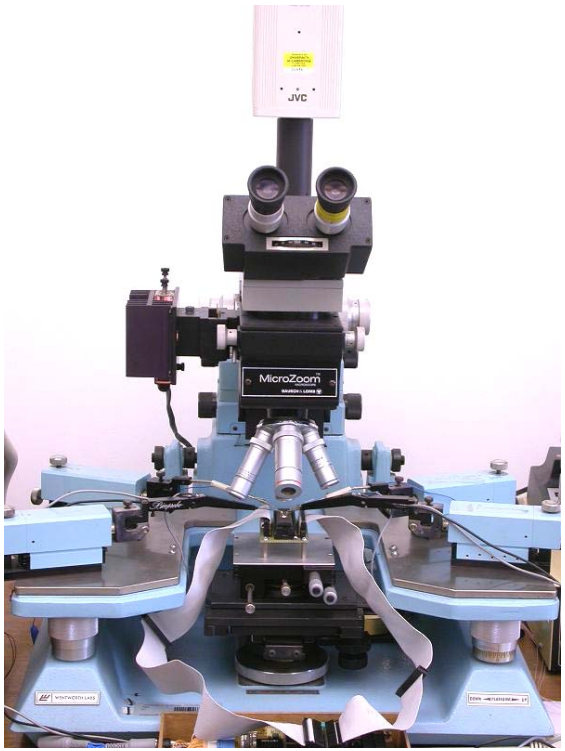


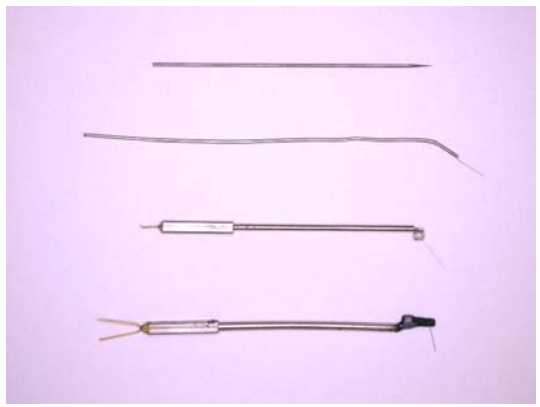
Confocal microscopes represent the different chip layers in different colors. In the right image, the metal interconnects have been removed with hydrofluoric acid. Both images together can be read almost as easily as a circuit diagram.

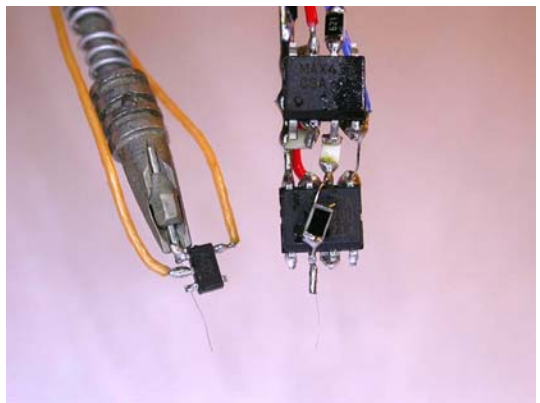
Picture courtesy of Dr Markus Kuhn

Invasive attacks

- Microprobing with fine electrodes
  - Eavesdropping on signals inside a chip
  - Injection of test signals and observing the reaction
  - Used for extraction of secret keys and memory contents

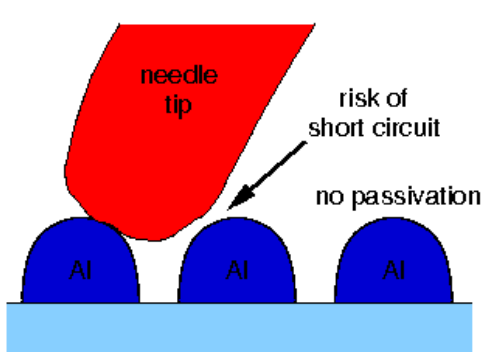


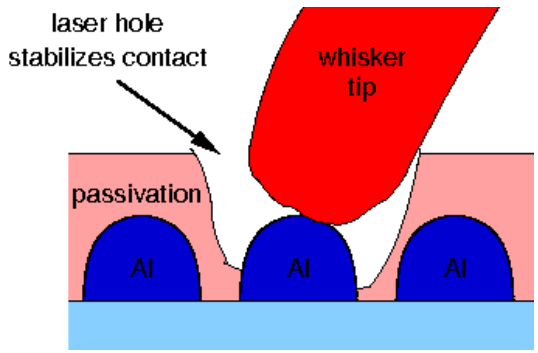




Invasive attacks

- Laser cutting systems
  - Removing polymer layer from a chip surface
  - Local removing of a passivation layer for microprobing attacks
  - Cutting metal wires inside a chip

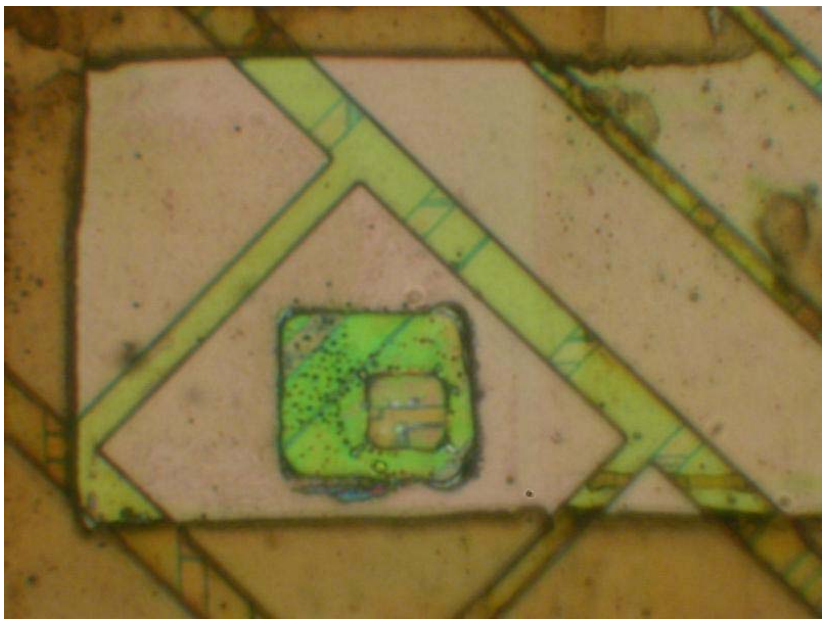


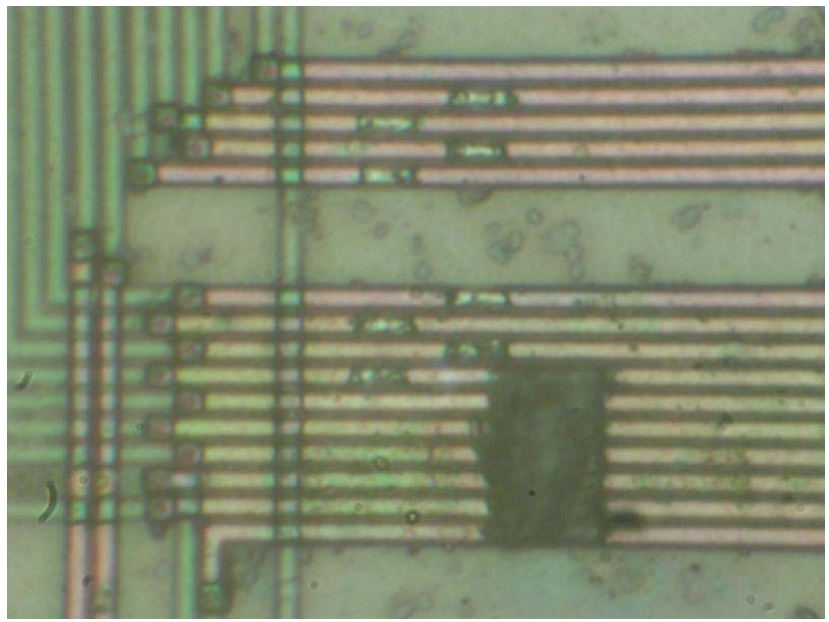


Picture courtesy of Dr Markus Kuhn

Invasive attacks

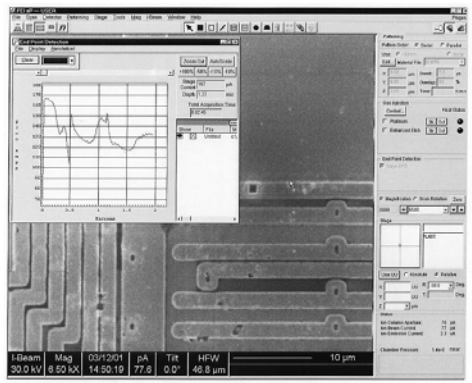
- Laser cutting systems
  - Removing polymer layer, cutting through M3 and M2 layers
  - Local removing of a passivation layer and cutting metal wires

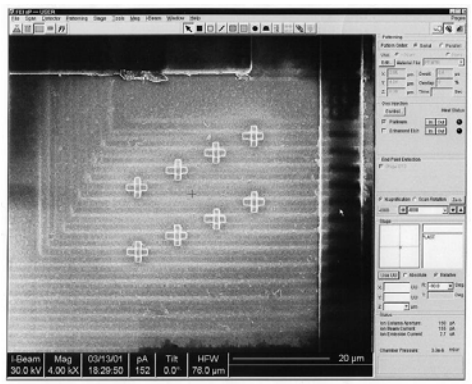




Invasive attacks

- Focused Ion Beam workstation
  - Chip-level surgery with 10 nm precision
  - Etching with high aspect ratio
  - Platinum and SiO_2 deposition

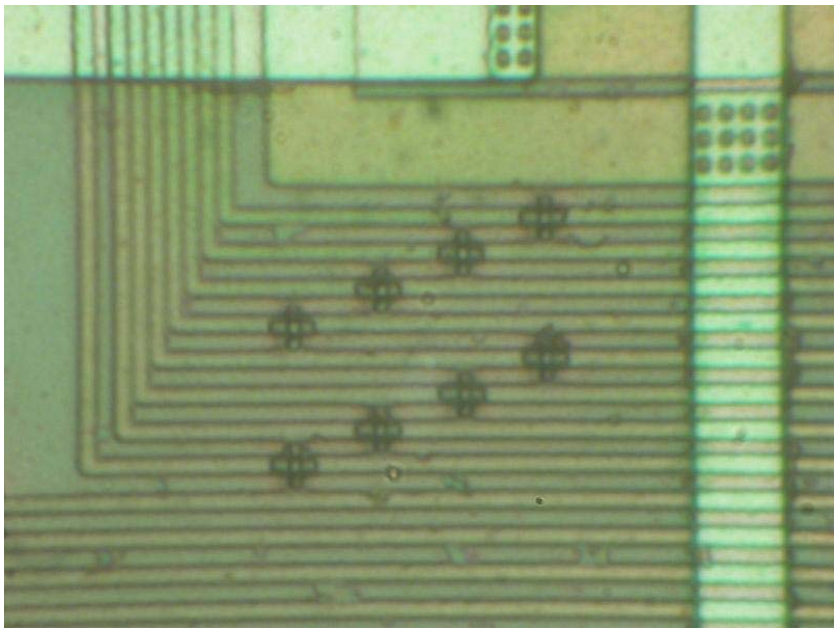


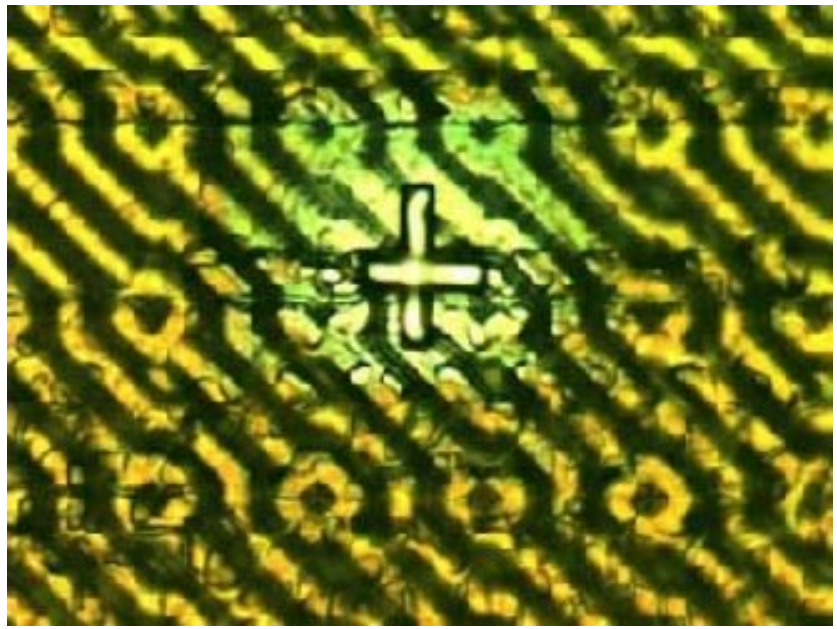


Picture courtesy of Semiresearch Ltd

Invasive attacks

- Focused Ion Beam workstation
  - Creating probing points inside smartcard chips
  - Modern FIBs allow access from the rear side; requires special backside chip preparation techniques to reduce the thickness of silicon to 10 – 20 µm

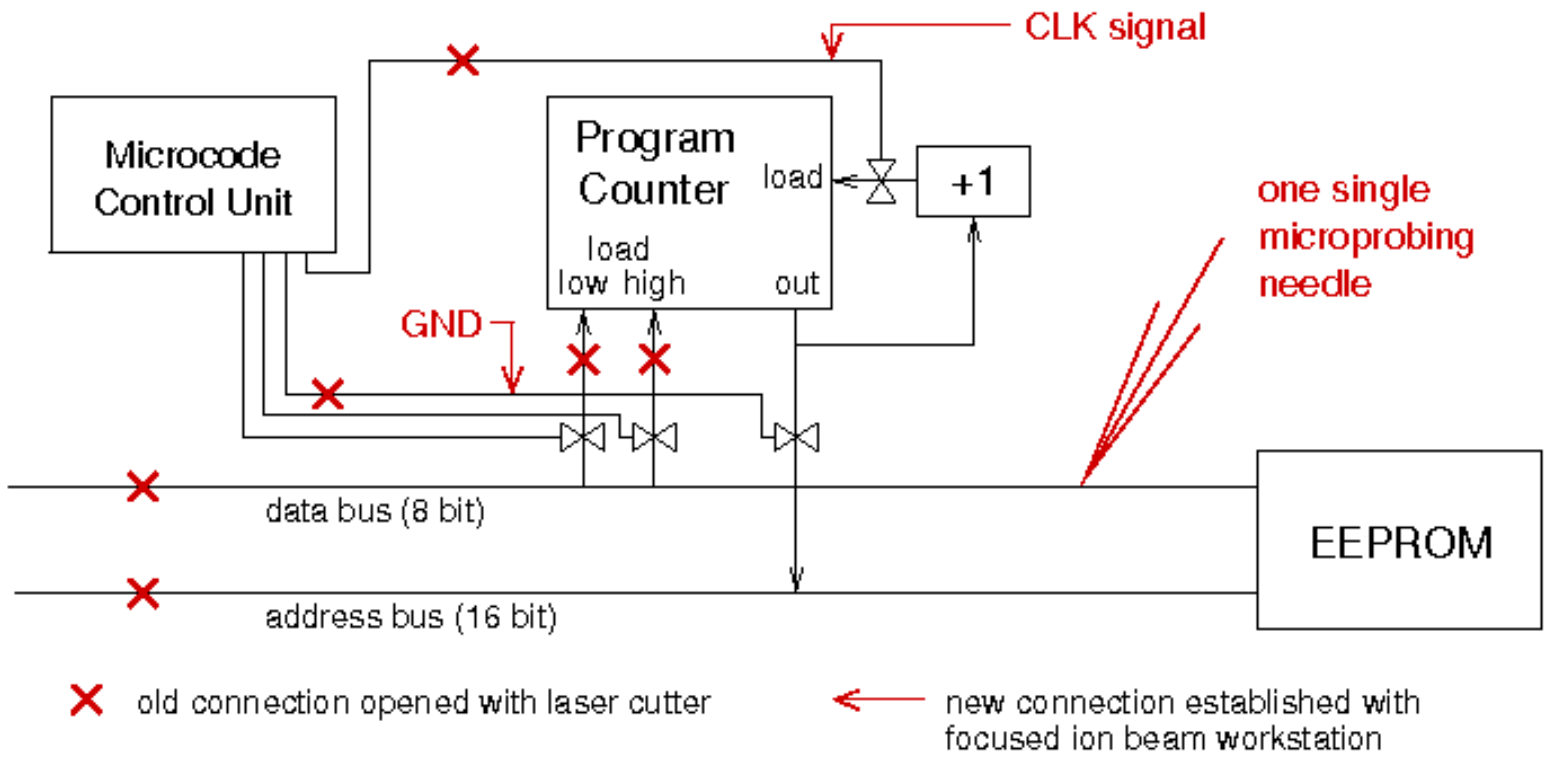




Picture: Oliver Kömmerling

Invasive attacks

- Chip modification
  - Reading out memory from smartcards
    - Disconnect most parts of the CPU except the program counter
    - Modify the program counter such that it will scan all addresses



Picture courtesy of Dr Markus Kuhn

Semi-invasive attacks

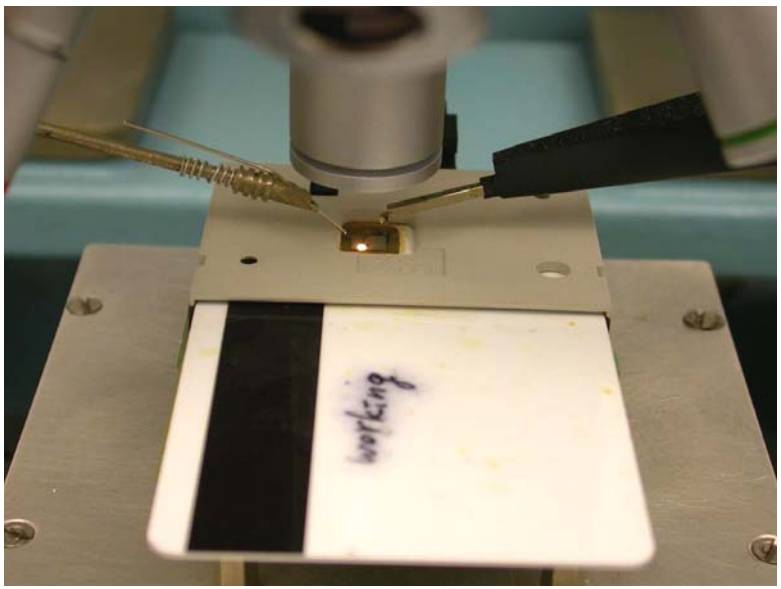
- Filling the gap between non-invasive and invasive attacks
  - Less damaging to target device (decapsulation without penetration)
  - Less expensive and easier to setup and repeat than invasive attacks
- Tools
  - IC soldering/desoldering station
  - Simple chemistry lab
  - Wire bonding machine
  - Signal generator, logic analyser and oscilloscope or PC with data acquisition board
  - High-resolution optical microscope
  - Special microscopes (laser scanning, infrared etc.)
  - UV light sources and lasers
  - Heating tools

Semi-invasive attacks

- History of semi-invasive attacks
  - UV attacks had been used for a long time before the semi-invasive method of attacks was defined
  - Advanced laser scanning techniques have been used in failure analysis to locate defects inside chips
  - We introduced optical fault injection attacks in 2002 as an example of a semi-invasive attack
- Sample preparation technique is very similar to the one used for invasive attacks – both front and rear-side decapsulation required
- Advanced optical probing techniques
- Yet to be explored
  - X-rays attacks (without even opening the chip package)
  - Interference with strong and localised electromagnetic fields

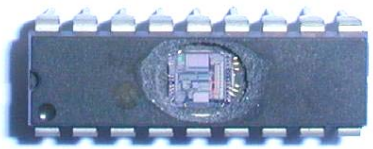
Semi-invasive attacks

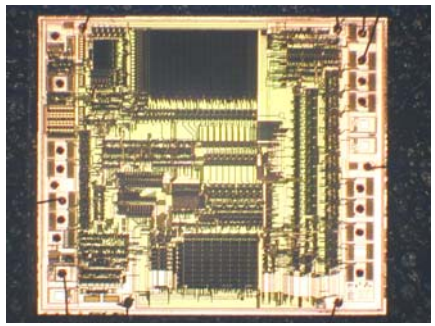
- Optical fault injection attacks
  - Optical fault injection was observed in my experiments with microprobing attacks in early 2001, introduced as new method in 2002
  - Lead to new powerful attack techniques and forced chip manufacturers to rethink their design and bring better protection
  - Original setup involved optical microscope with a photoflash

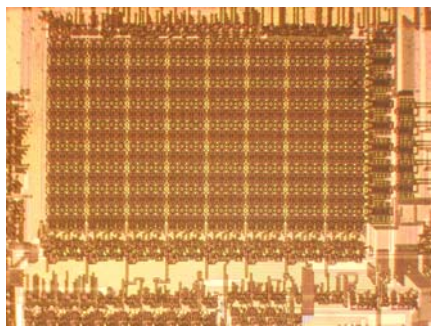


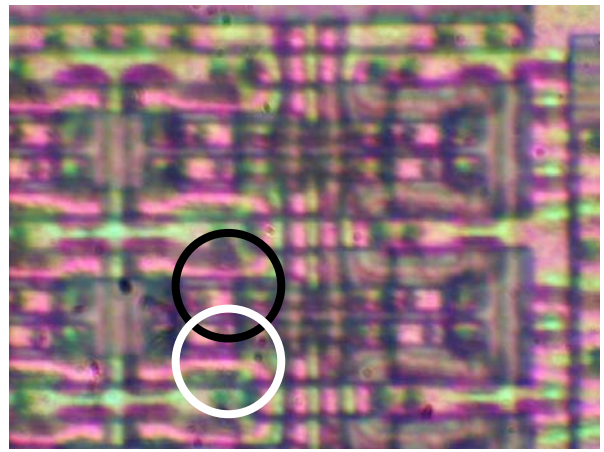
Semi-invasive attacks

- Optical fault injection attack setup
  - The Microchip PIC16F84 microcontroller (1.2 μm fabrication process) was programmed to monitor its internal SRAM
  - The chip was decapsulated and placed under a microscope
  - Magnification of the microscope was set to its maximum (1500×)
  - Light from the photoflash was shaped with aluminium foil aperture



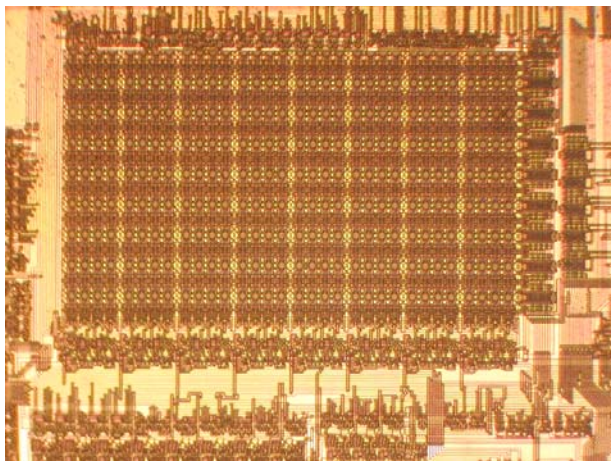






Semi-invasive attacks

- Optical fault injection attacks
  - Allocation of memory bits inside the array
  - Physical location of each memory address
  - Modifying memory contents

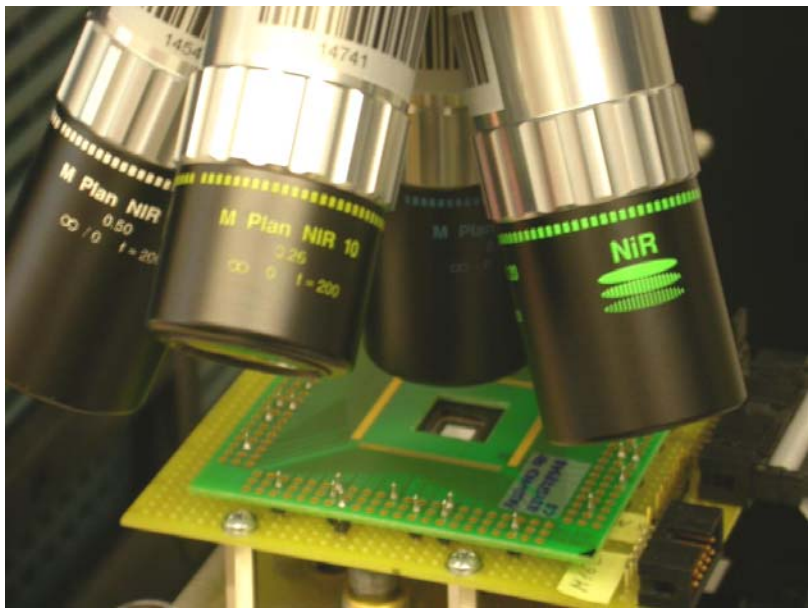


BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0

30h	34h	38h	3Ch	40h	44h	48h	4Ch	10h	14h	18h	1Ch	20h	24h	28h	2Ch	0Ch
31h	35h	39h	3Dh	41h	45h	49h	4Dh	11h	15h	19h	1Dh	21h	25h	29h	2Dh	0Dh
32h	36h	3Ah	3Eh	42h	46h	4Ah	4Eh	12h	16h	1Ah	1Eh	22h	26h	2Ah	2Eh	0Eh
33h	37h	3Bh	3Fh	43h	47h	4Bh	4Fh	13h	17h	1Bh	1Fh	23h	27h	2Bh	2Fh	0Fh

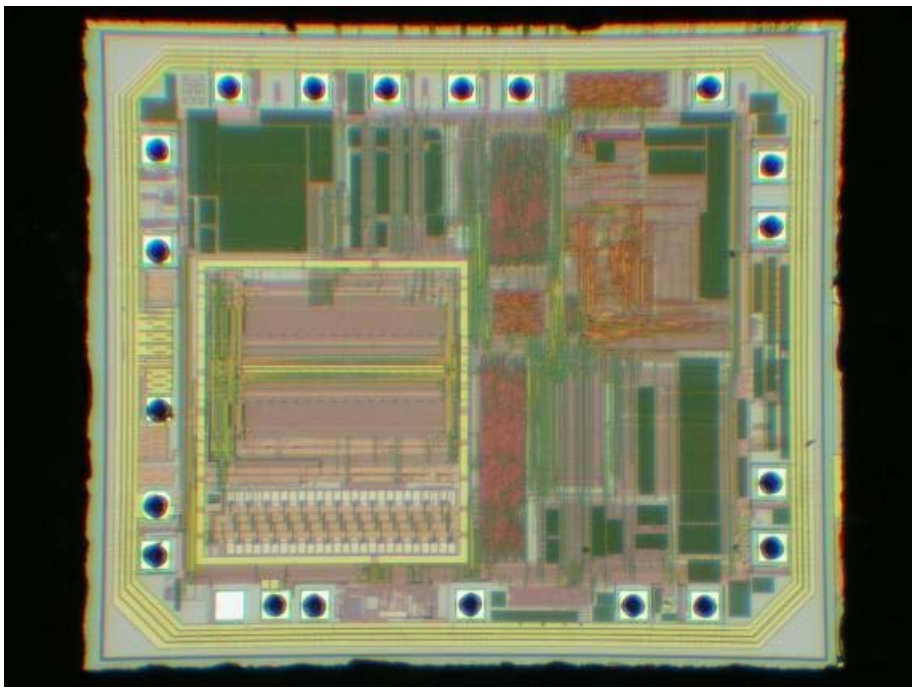
Semi-invasive attacks

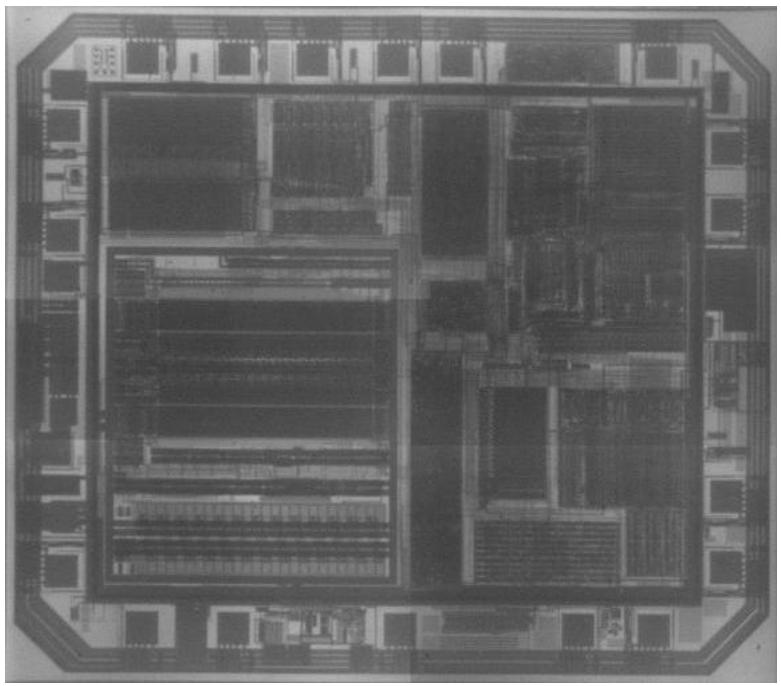
- Backside infrared imaging
  - Microscopes with IR optics should be used
  - IR enhanced CCD cameras or special cameras must be used
  - Resolution is limited to 0.6 μm by the wavelength of used light



Semi-invasive attacks

- Backside infrared imaging
  - View is not obstructed by multiple metal layers
  - Reflected and transmitted light illumination can be used

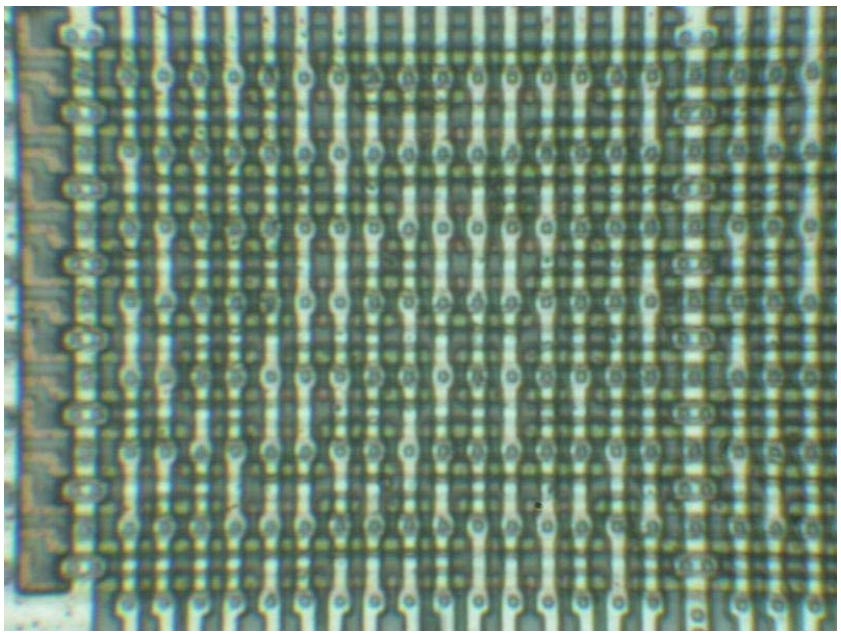


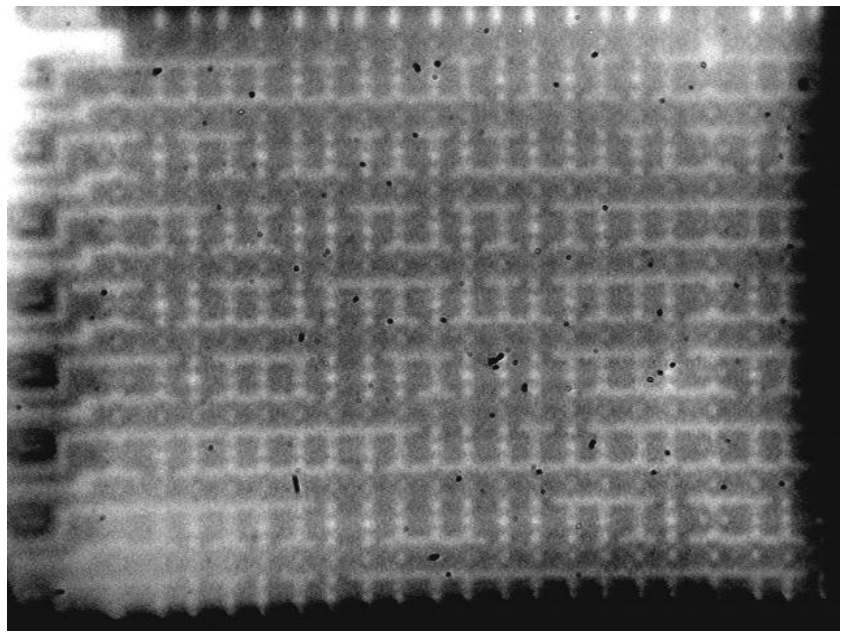


Texas Instruments MSP430F112 microcontroller

Semi-invasive attacks

- Backside infrared imaging
  - Mask ROM extraction without chemical etching
    - Resolution is limited by wavelength of the infrared light

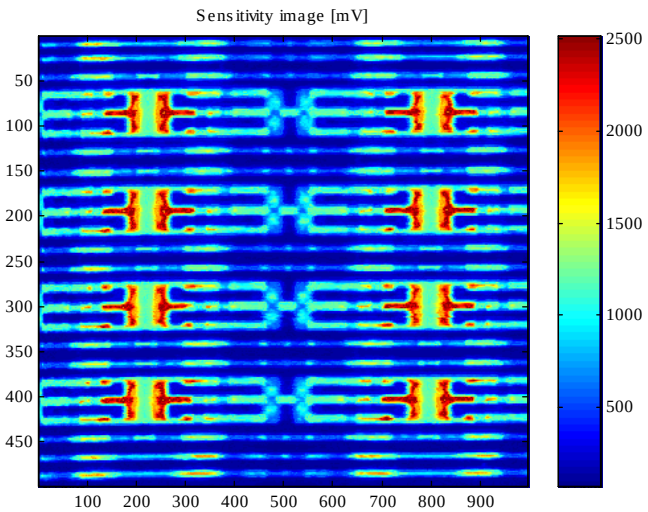


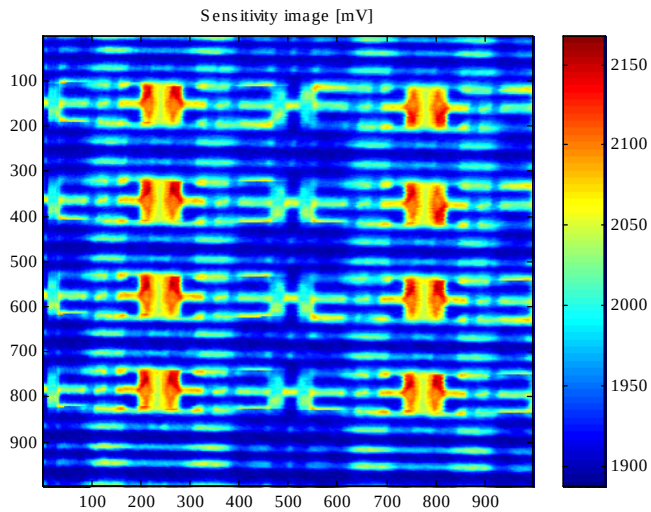


Motorola MC68HC705P6A microcontroller

Semi-invasive attacks

- Advanced imaging techniques – active photon probing
  - Light-induced current variation
    - Alternative to light-induced voltage alteration (LIVA) technique
    - Photon-induced photocurrent is dependable from the state of a transistor
    - Reading logic state of CMOS transistors inside a powered-up chip
    - Works from the rear side of a chip (using infrared lasers)

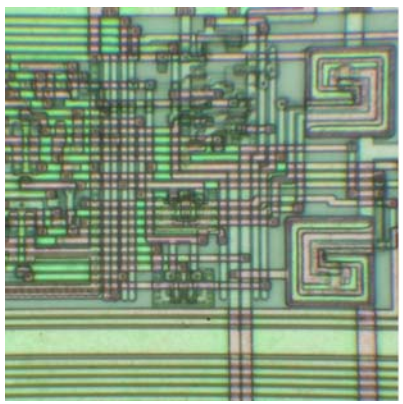


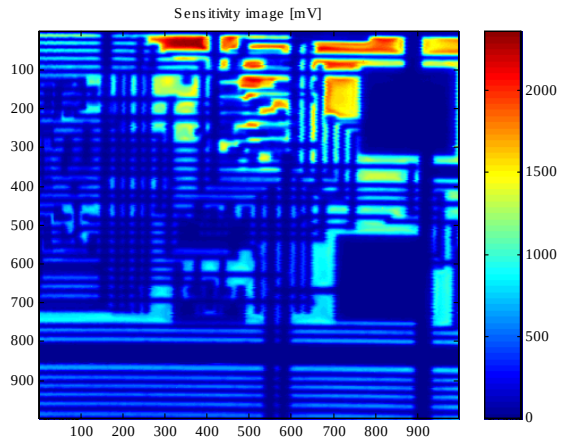


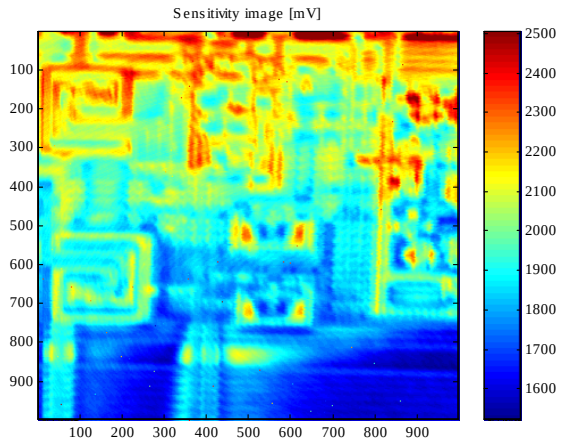
Microchip PIC16F84 microcontroller

Semi-invasive attacks

- Advanced imaging techniques – active photon probing
  - Optical Beam Induced Current (OBIC)
    - Photons with energy exceeding semiconductor band gap ionize IC's regions, which results in a photocurrent flow used to produce the image
    - Localisation of active areas
    - Also works from the rear side of a chip (using infrared lasers)



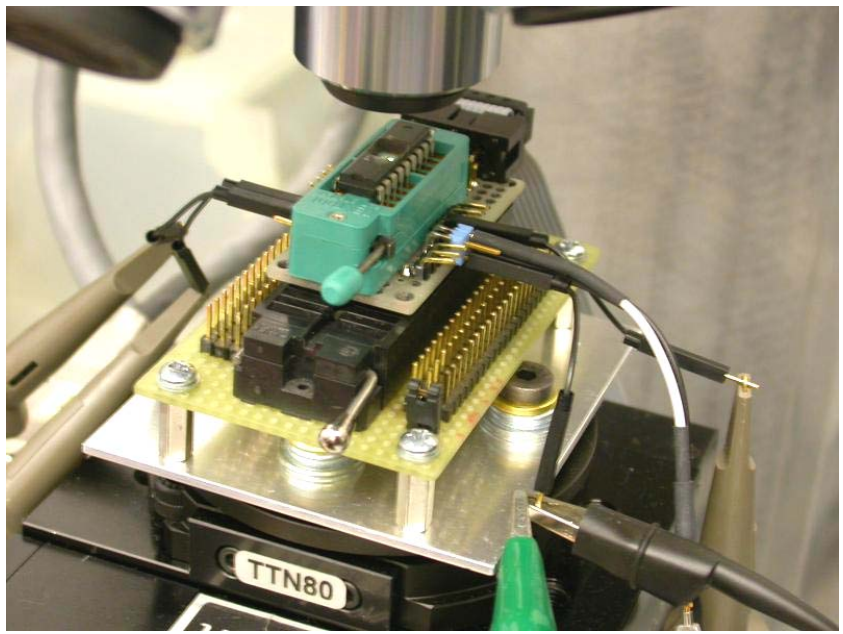




Microchip PIC16F84A microcontroller

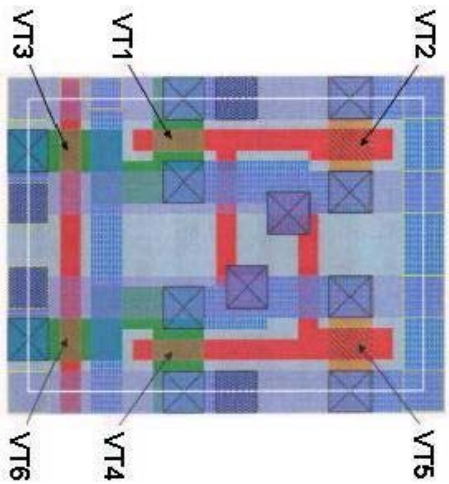
Semi-invasive attacks

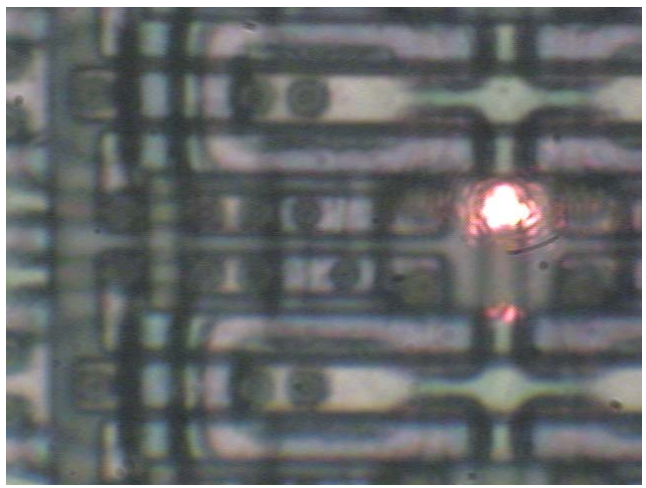
- Optically enhanced position-locked power analysis
  - Microchip PIC16F84 microcontroller
  - Classic power analysis setup (10 Ω resistor in GND, digital storage oscilloscope) plus laser microscope system setup

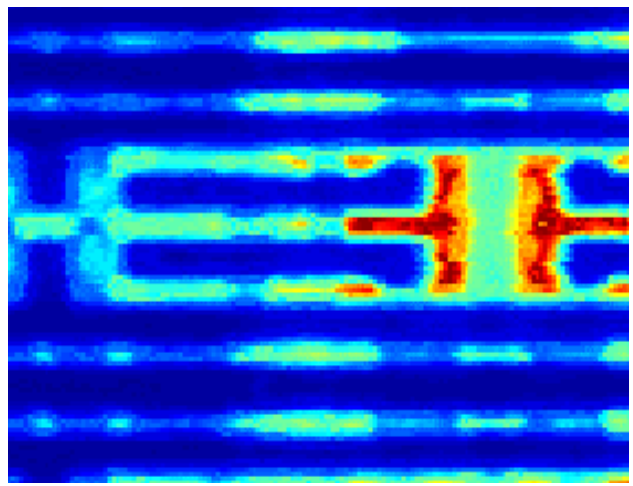


Semi-invasive attacks

- Optically enhanced position-locked power analysis
  - Standard laser scanning operation reveals all sensitive areas
  - Microcontroller was programmed with the program which accesses certain memory locations and output result to the ports
  - Test pattern
    - Run the code inside the microcontroller and store the power trace
    - Trigger the fault injection event and store the power trace
    - Compare two traces

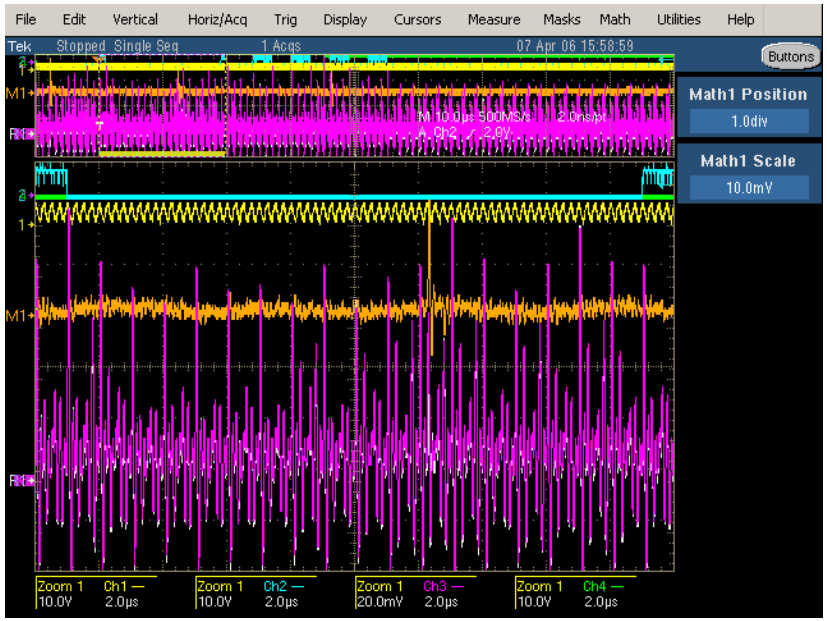






Semi-invasive attacks

- Optically enhanced position-locked power analysis
  - Results for memory read operations
    - Non-destructive analysis of active memory locations (‘0’ and ‘1’)
  - Results for memory write operations
    - Non-destructive analysis of active memory locations (‘0→0’, ‘0→1’, ‘1→0’ and ‘1→1’)



Semi-invasive attacks

- Compared with invasive attacks

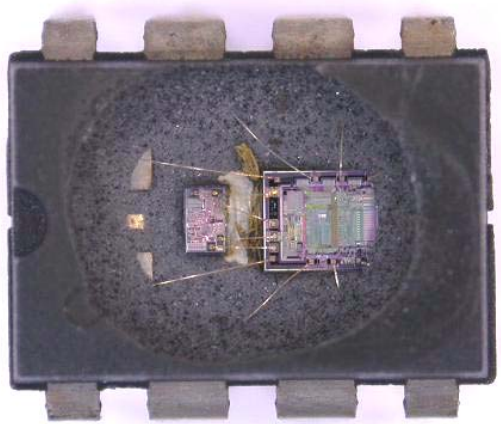
INVASIVE	SEMI-INVASIVE
Microprobing	Laser scanning Optical probing
Chip modification (laser cutter or FIB)	Fault injection
Reverse engineering	Special microscopy
Rear-side approach with a FIB	Infrared techniques

- Compared with non-invasive attacks

NON-INVASIVE	SEMI-INVASIVE
Power and clock glitching	Fault injection
Power analysis	Special microscopy Optical probing

Defence technologies

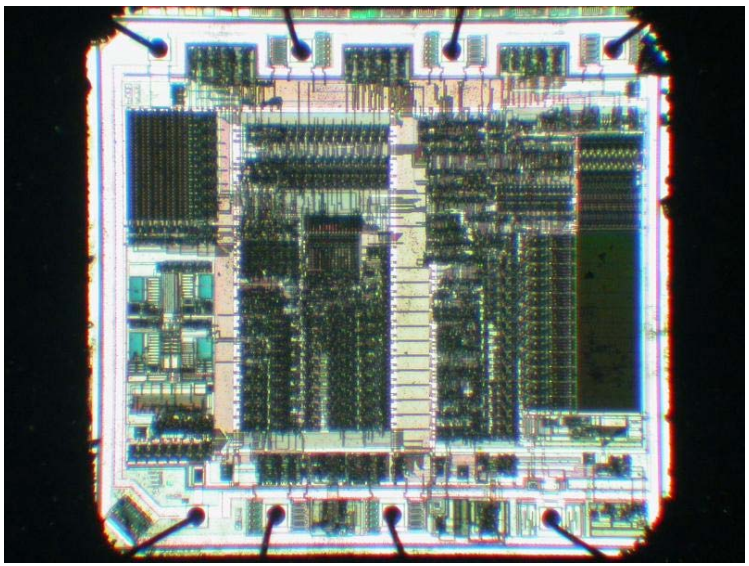
- Tamper protection level MODL
  - Hiding
  - Restricted access



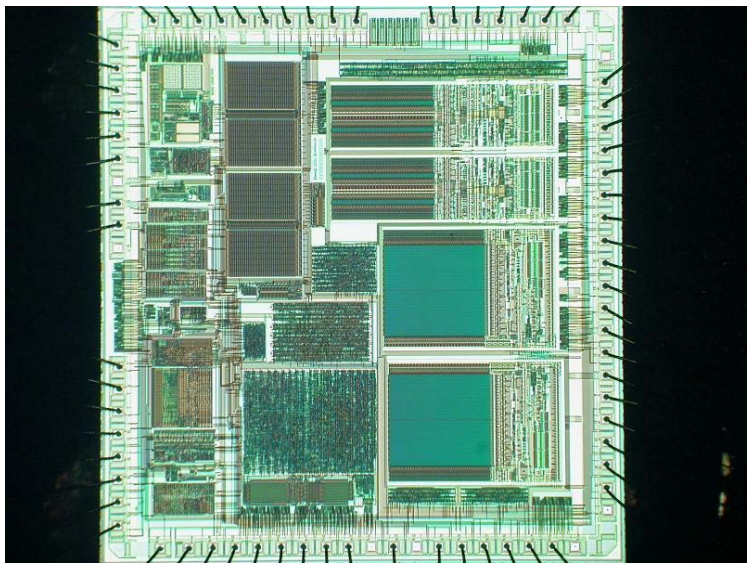
Microchip PIC12CE518 microcontroller

Defence technologies

- Tamper protection level MOD
  - Security fuse is placed separately from the memory array (easy to locate and defeat)
  - Security fuse is embedded into the program memory (hard to locate and defeat), similar approach is used in many smartcards in the form of password protection and encyption keys



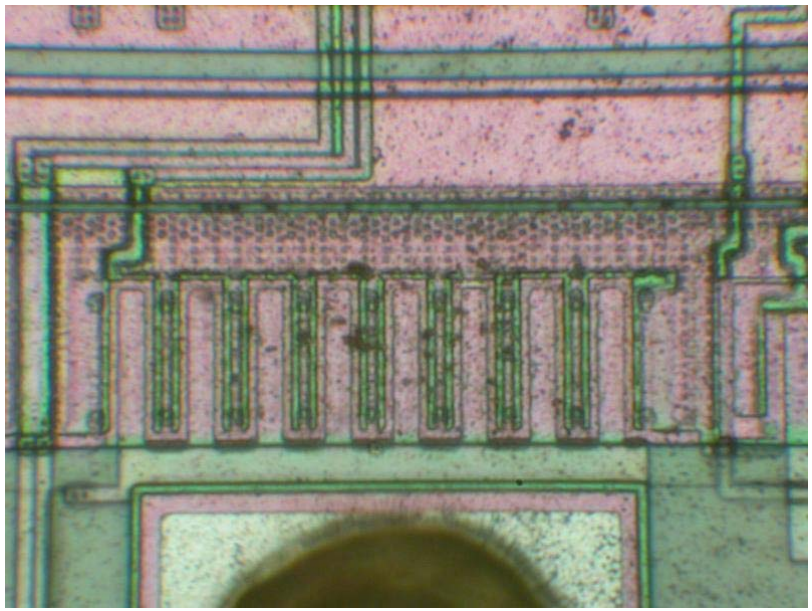
Microchip PIC12C508 microcontroller



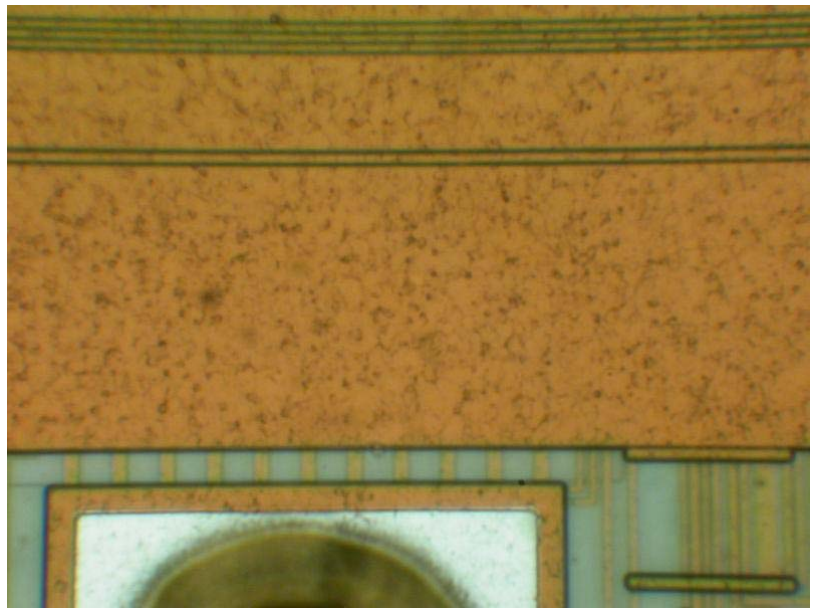
Motorola MC68HC908AZ60A microcontroller

Defence technologies

- Tamper protection level MOD
  - Planarisation as a part of modern chip fabrication processes (0.5 µm or smaller feature size)



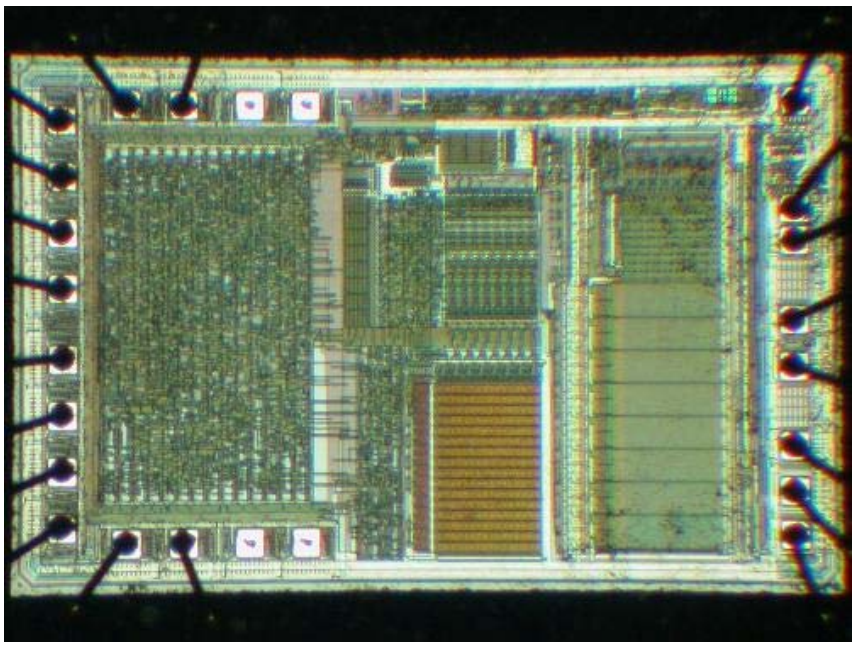
Microchip PIC16F877 microcontroller



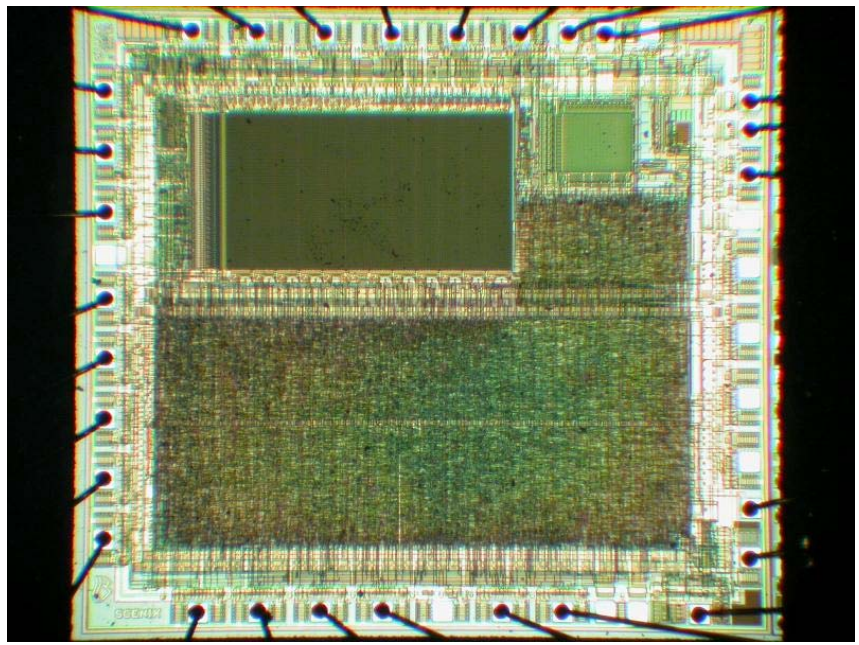
Microchip PIC16F877A microcontroller

Defence technologies

- Tamper protection level MOD
  - Removing obvious ways to trace the data and security protection
  - Glue logic design (used in modern microcontrollers and smartcards)



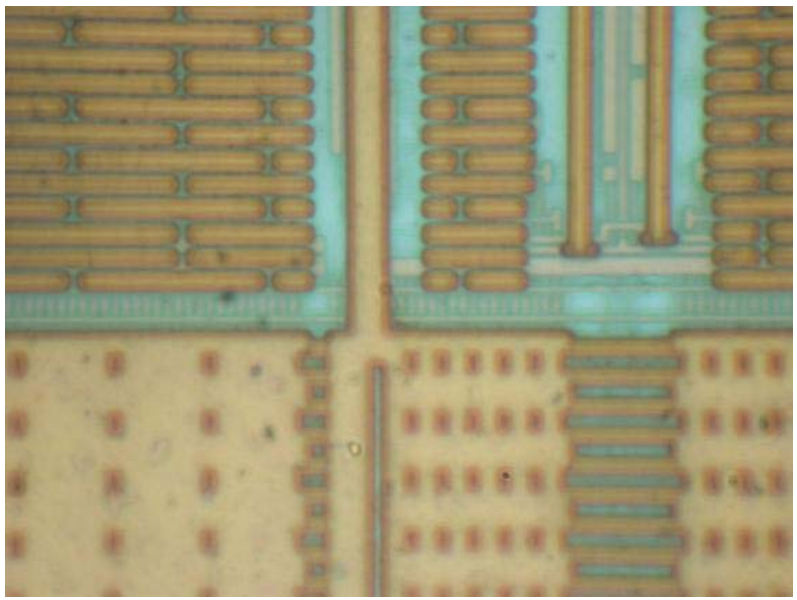
Cypress CY7C63001A microcontroller



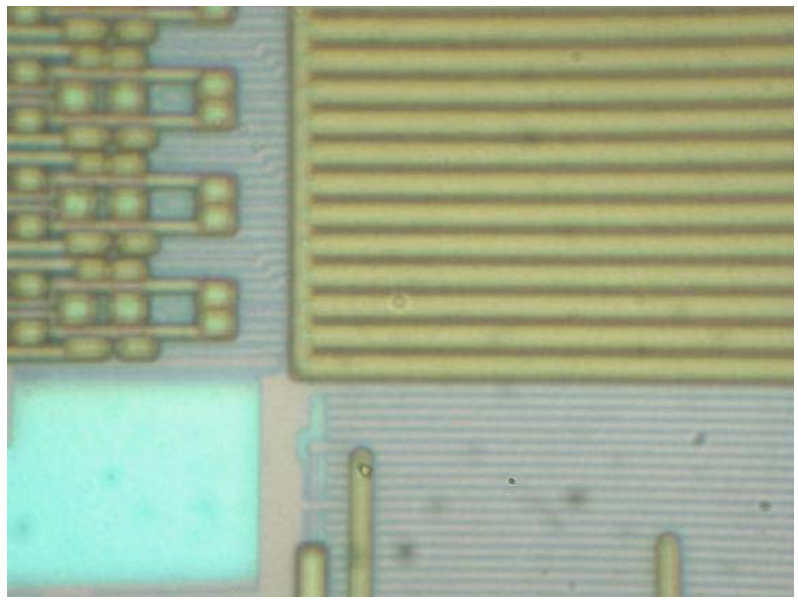
Scenix SX28 microcontroller

Defence technologies

- Tamper protection level MOD
  - Fabrication process reduced to under 0.5 μm
  - Multiple metal layers obstruct direct observation
  - Increased complexity of circuits



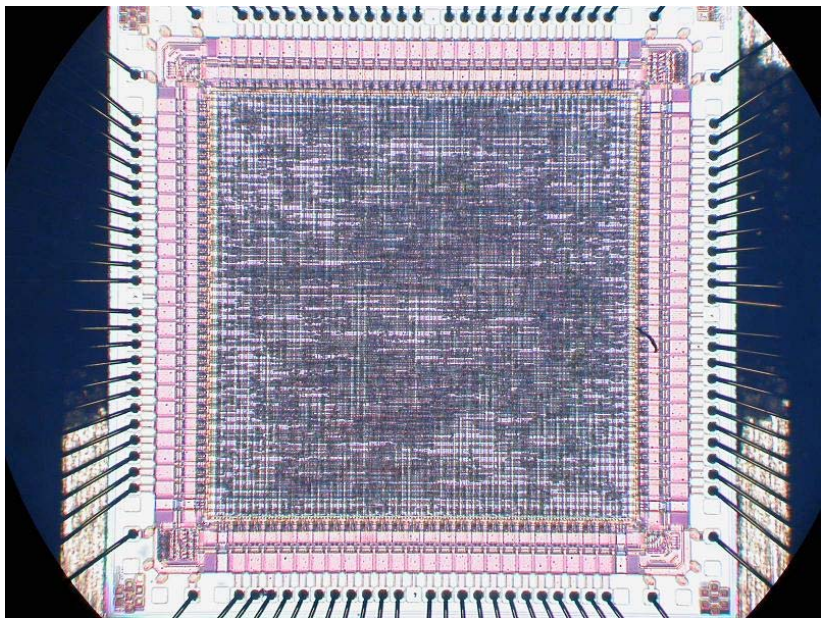
Atmel ATmega16 microcontroller

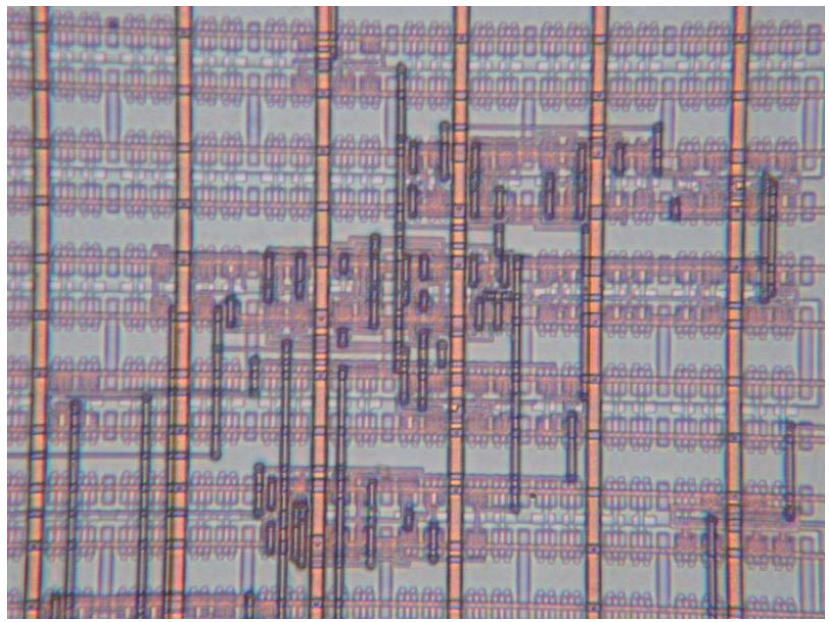


Motorola MC68HC908AP16 microcontroller

Defence technologies

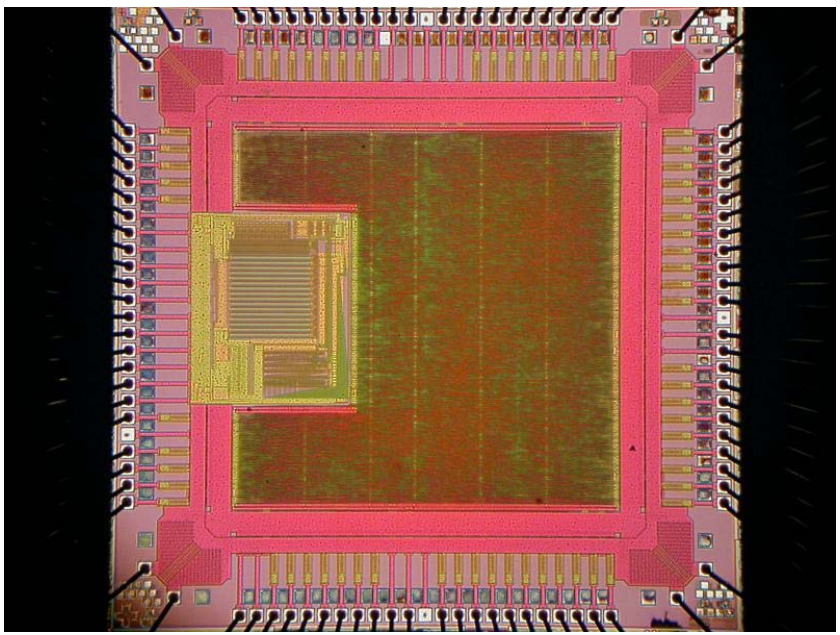
- Tamper protection level MOD to MODH
  - Application Specific Integrated Circuits (ASIC)
    - Built from libraries using one or two factory programmable metal layers (very similar to Mask ROM fabrication)
    - Can be reverse engineered, but it is very tedious and expensive process

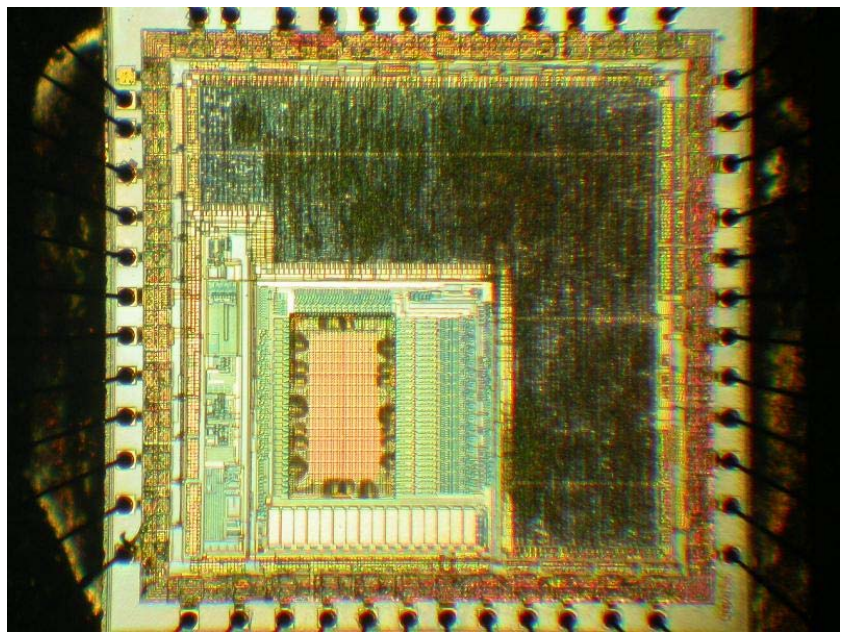




Defence technologies

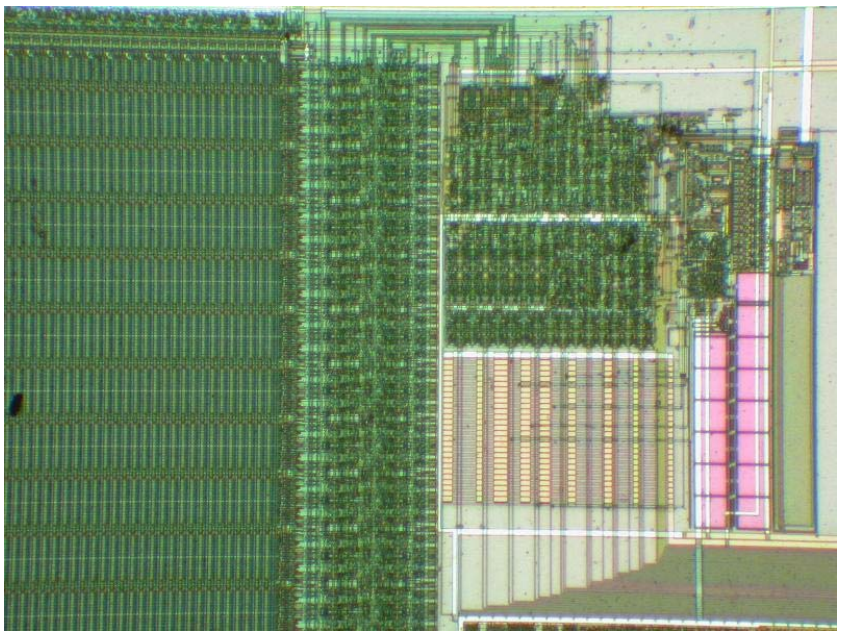
- Tamper protection level MODH
  - Custom designed Integrated Circuits
    - Glue logic design from VHDL or logic level (Netlist)
    - Fully custom design with security requirements
    - Reverse engineering is extremely expensive and long process





Defence technologies

- Tamper protection level MODH
  - Memory management
  - Bus encryption
    - Simple algorithms not to slow down the communication

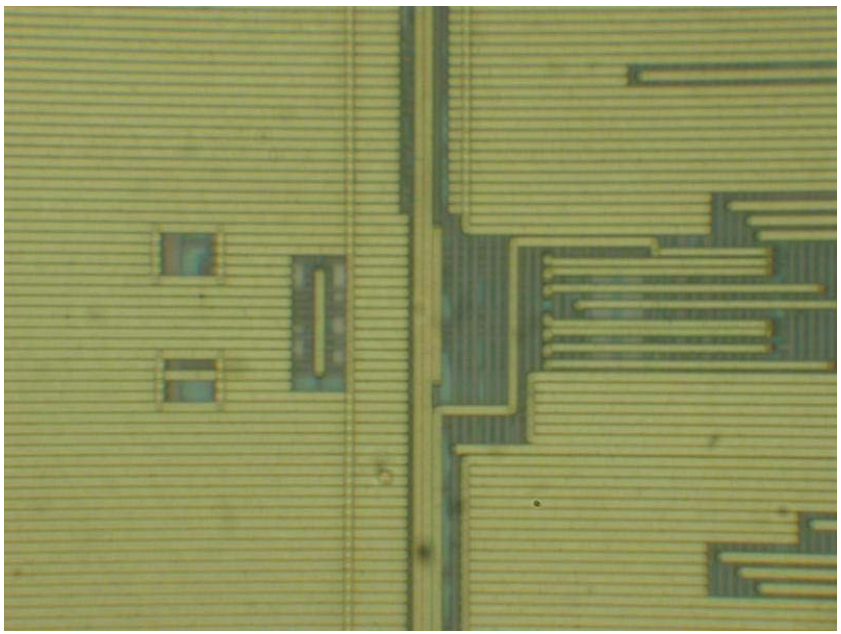


Infineon SLE66 smartcard

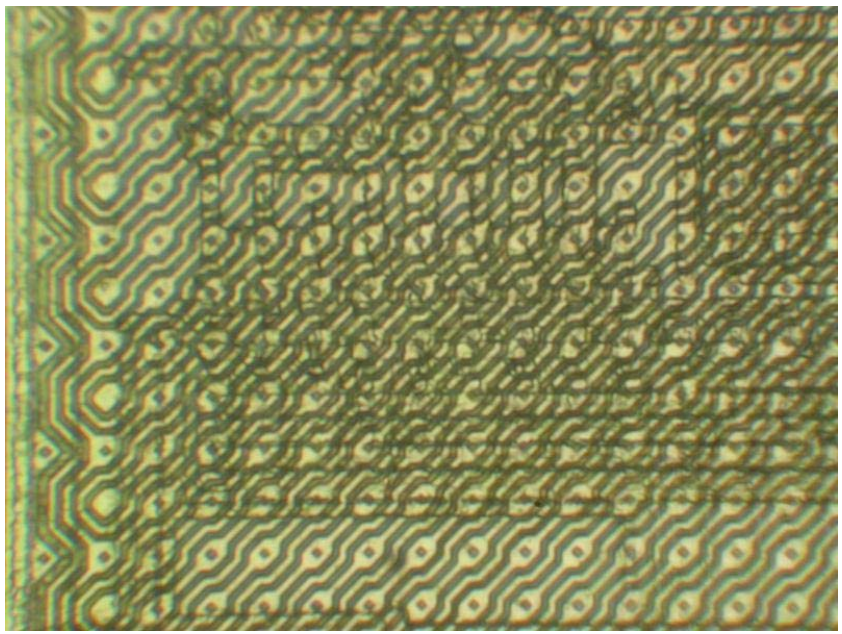
Dallas Semiconductor DS5002FP microcontroller

Defence technologies

- Tamper protection level MODH
  - Top metal layers with sensors
  - Voltage, frequency and temperature sensors
  - Memory access protection, crypto-coprocessors
  - Internal clocks, power pumps and asynchronous logic design



Temic T89C51RD2 microcontroller



STMicroelectronics ST16 smartcard

Defence technologies

- Tamper protection level HIGH
  - Tamper protection enclosures
    - Give highest possible protection against invasive attacks
    - Not very compact, require constant battery power supply
    - High cost compared to silicon solution

Pictures courtesy of Dr Markus Kuhn

Conclusions

- There is no such a thing as absolute protection
  - Given enough time and resources any protection can be broken
- Technical progress helps a lot, but has certain limits
  - Do not overestimate capabilities of the silicon circuits
  - Do not underestimate capabilities of the attackers
- Defence should be adequate to anticipated attacks
  - Security hardware engineers must be familiar with attack technologies to develop adequate protection
  - Choosing the correct protection saves money in development and manufacturing
- Attack technologies are constantly improving, so should the defence technologies
- Many vulnerabilities were found in various secure chips and more are to be found posing more challenges to hardware security engineers