

---

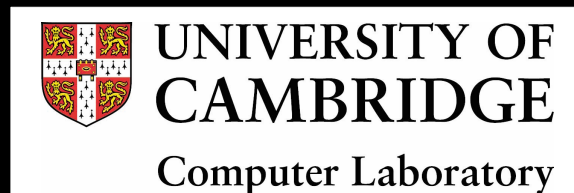
# Tamper resistance and physical attacks

Part II: Attack technologies

Dr Sergei Skorobogatov

*<http://www.cl.cam.ac.uk/~sps32>*

*email: [sps32@cam.ac.uk](mailto:sps32@cam.ac.uk)*



Security Group, TAMPER Lab

# Non-invasive attacks

---

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

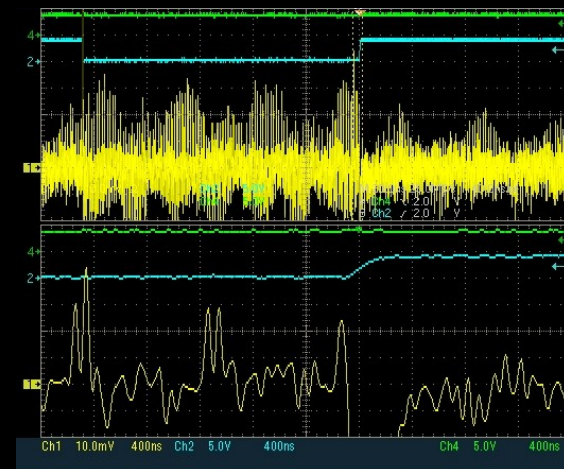
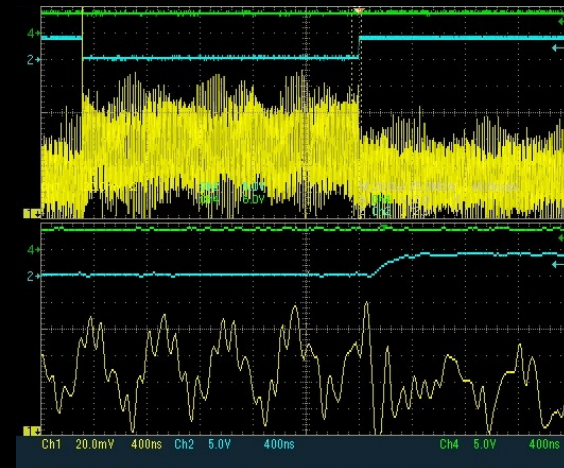
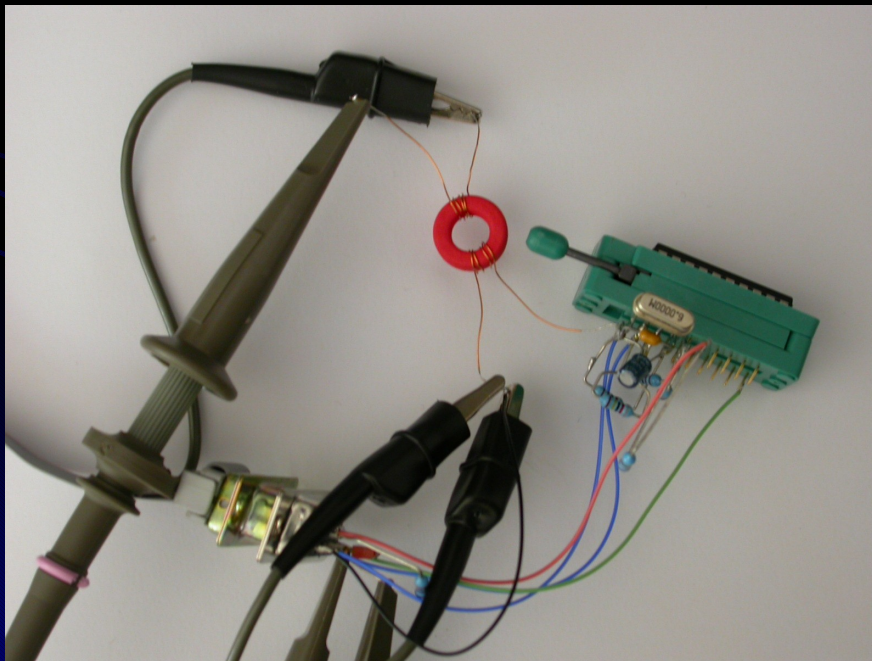
# Non-invasive attacks

---

- **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
  - Forcing a device into test mode

# Non-invasive attacks

- Power analysis
  - Measuring power consumption in time (voltage drop over a resistor or using a transformer)



# Non-invasive attacks

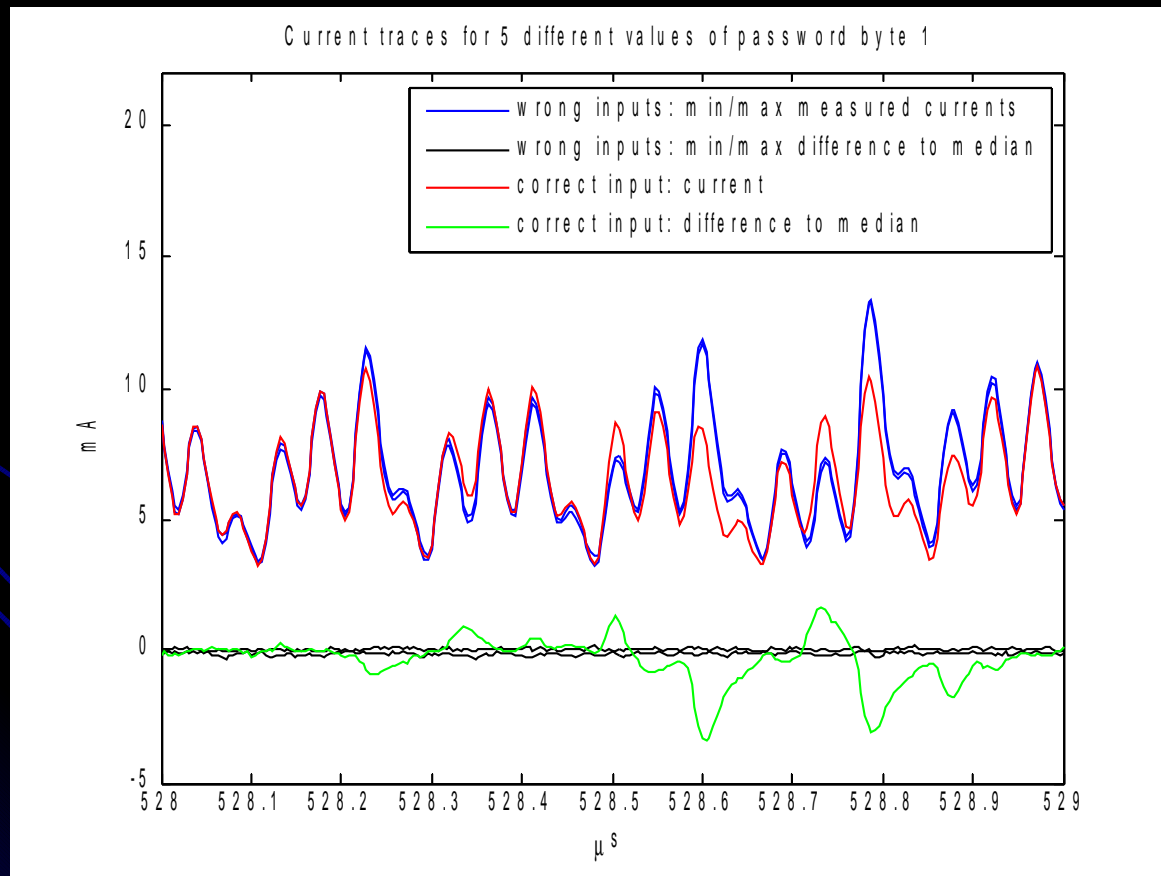
---

- **Power analysis**
  - 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
  - When a difference in a single bit of data is required, average over hundreds or thousands of power traces is necessary
  - To find a difference in an instruction flaw, a single trace acquired with a high resolution is enough
  - There are some tricks to reduce the noise
    - PCB design
    - Low-noise components
    - Oversampling or high-resolution acquisition

# Non-invasive attacks

## Power analysis

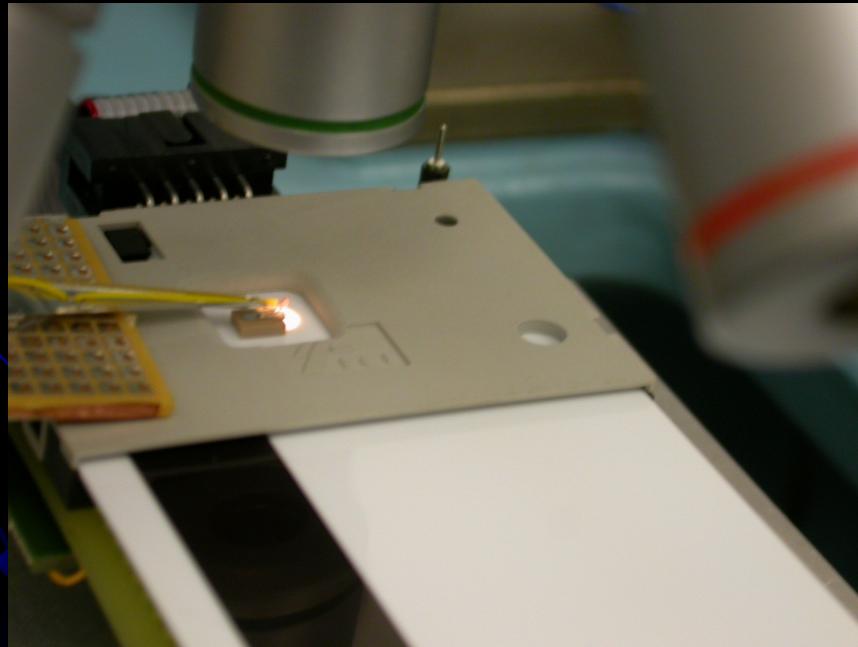
- Password check in Freescale MC908AZ60A microcontroller
- Single acquisition, 250 Ms/s (10 MHz CPU clock):



# Non-invasive attacks

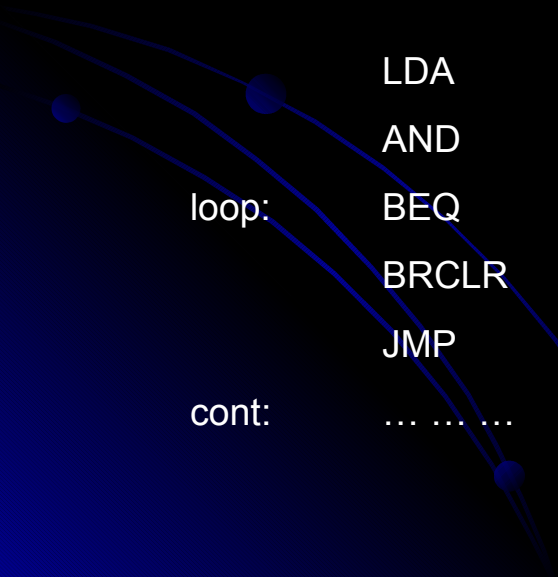
---

- **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 (1.8 – 2.2 V) power glitching (standard  $V_{DD} = 5\text{ V}$ )

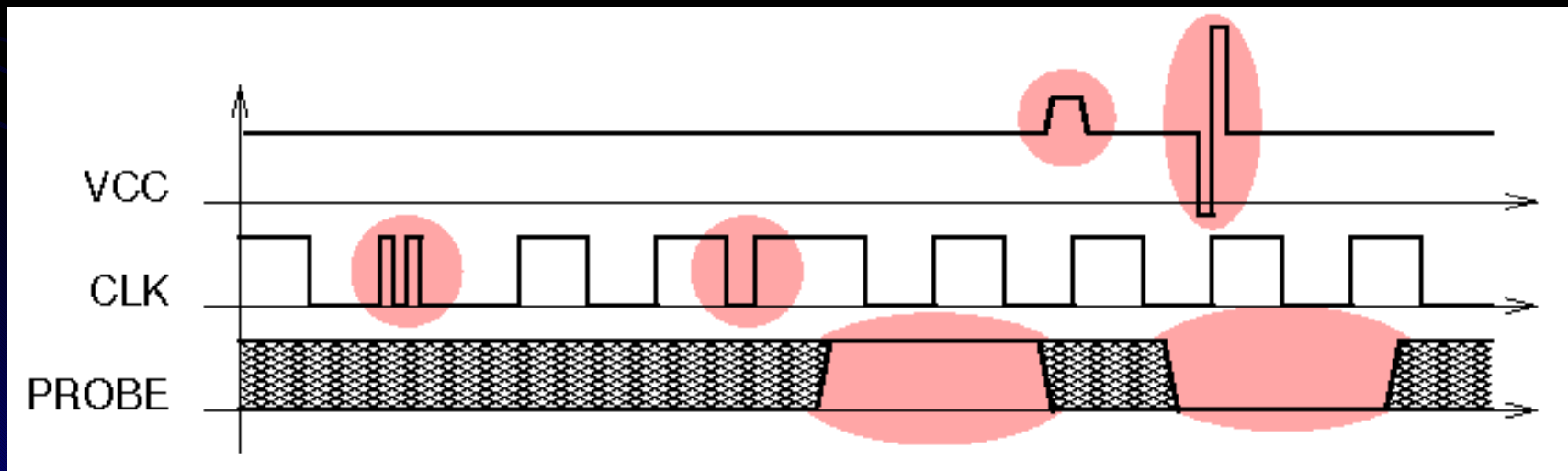


```
LDA    #01h
AND    $0100    ;the contents of the EEPROM byte is checked
loop:  BEQ    loop    ;endless loop if bit 0 is zero
       BRCLR  4, $0003, cont    ;test mode of operation
       JMP    $0000    ;direct jump to the preset address
cont:  ... ..
```



# Non-invasive attacks

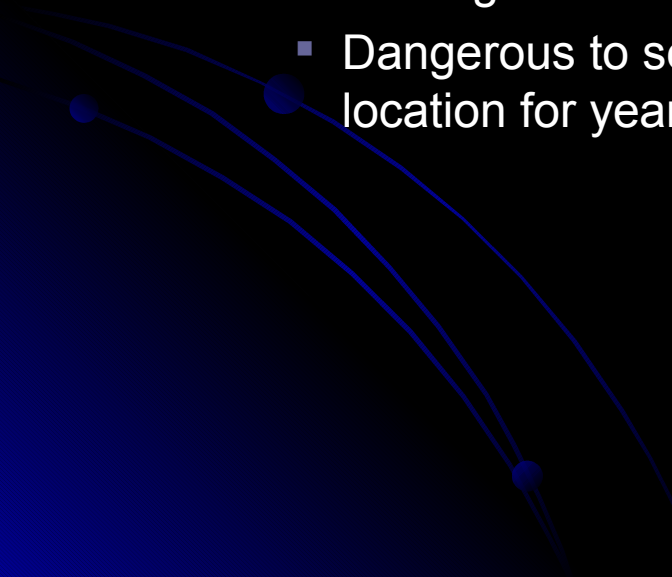
- Glitch attacks
  - Change single instructions or data
    - Links between gates form RC delay elements. Maximum RC sum of any signal path determines maximum CLK frequency
    - Transistors compare internal signals with a part of  $V_{CC}$  (usually  $\frac{1}{2}$ ), which allows  $V_{CC}$  glitches



Picture courtesy of Dr Markus Kuhn

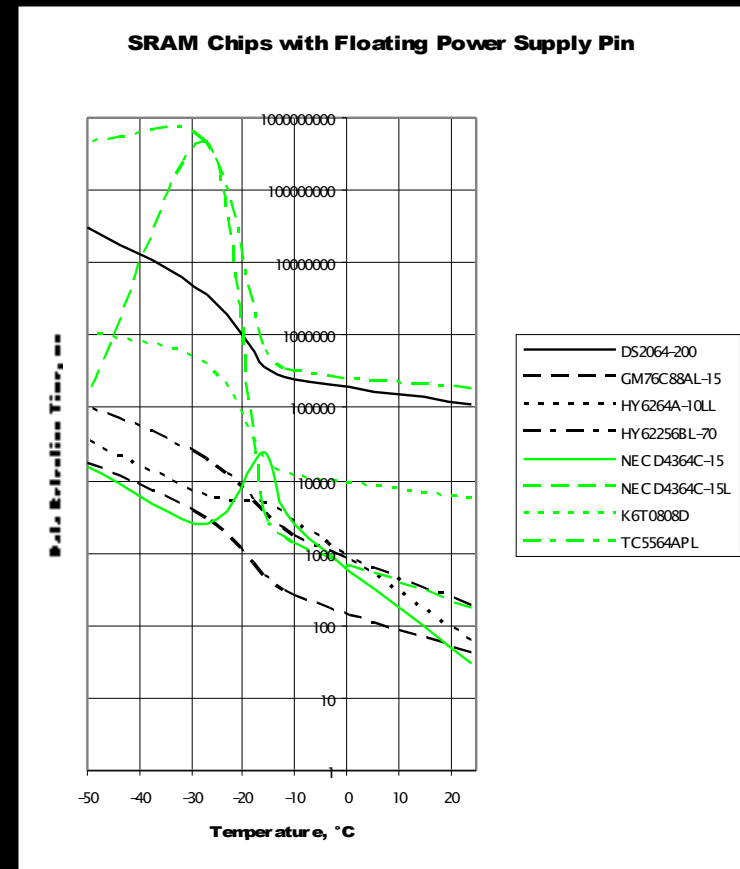
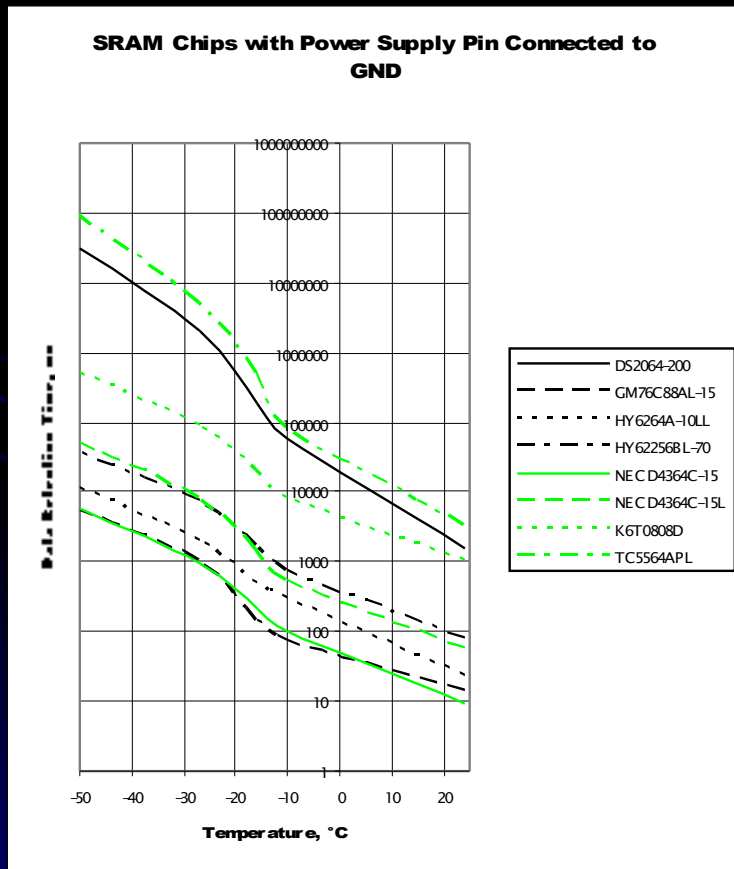
# Non-invasive attacks

---

- 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 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



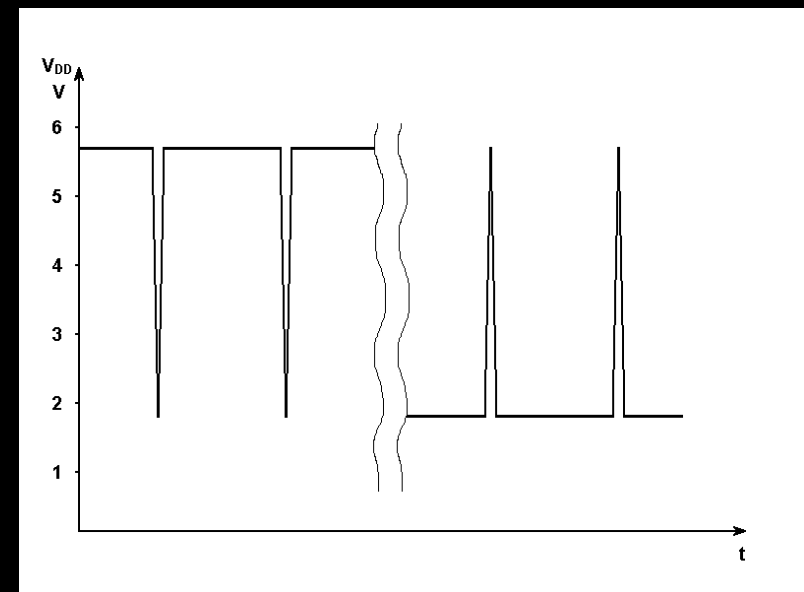
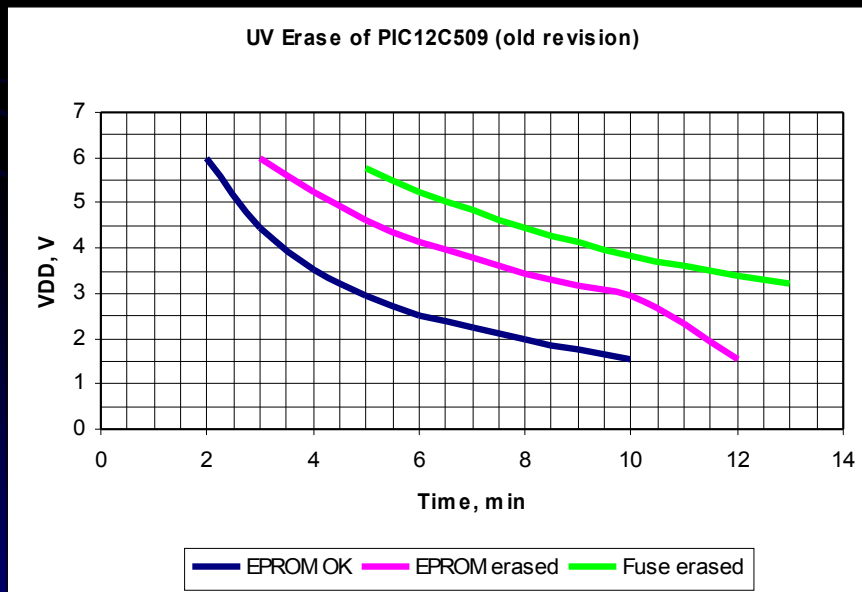
# Non-invasive attacks

---

- Data remanence in non-volatile memories
  - EPROM, EEPROM and Flash
    - Widely used in microcontrollers and smartcards
    - Floating-gate transistors,  $10^3 - 10^5 e^-$ ,  $\Delta V_{TH} \sim 3.5 V$
  - Levels of remanence threat
    - File system (erasing a file  $\rightarrow$  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

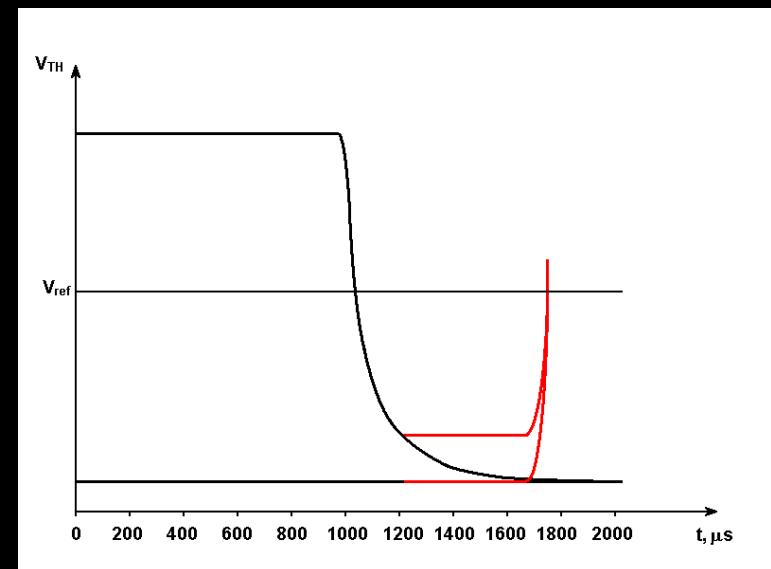
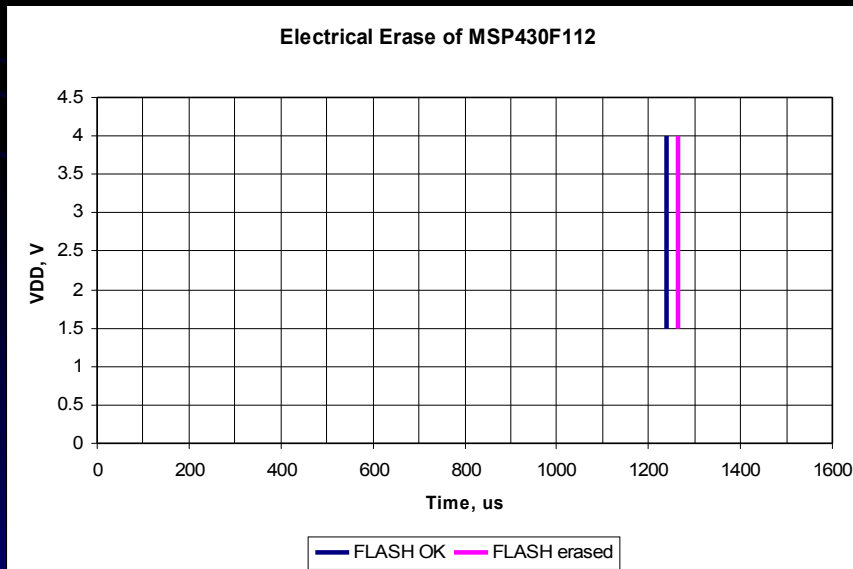
# Non-invasive attacks

- Data remanence in EPROM, EEPROM and Flash
  - UV light or electrical erase followed by power glitching
  - Memory and password/fuse are erased simultaneously
    - $V_{DD}$  variation or power glitching
    - Read sense circuit:  $V_{TH} = K V_{DD}$ ,  $K \sim 0.5$
  - Not suitable for modern semiconductor technologies



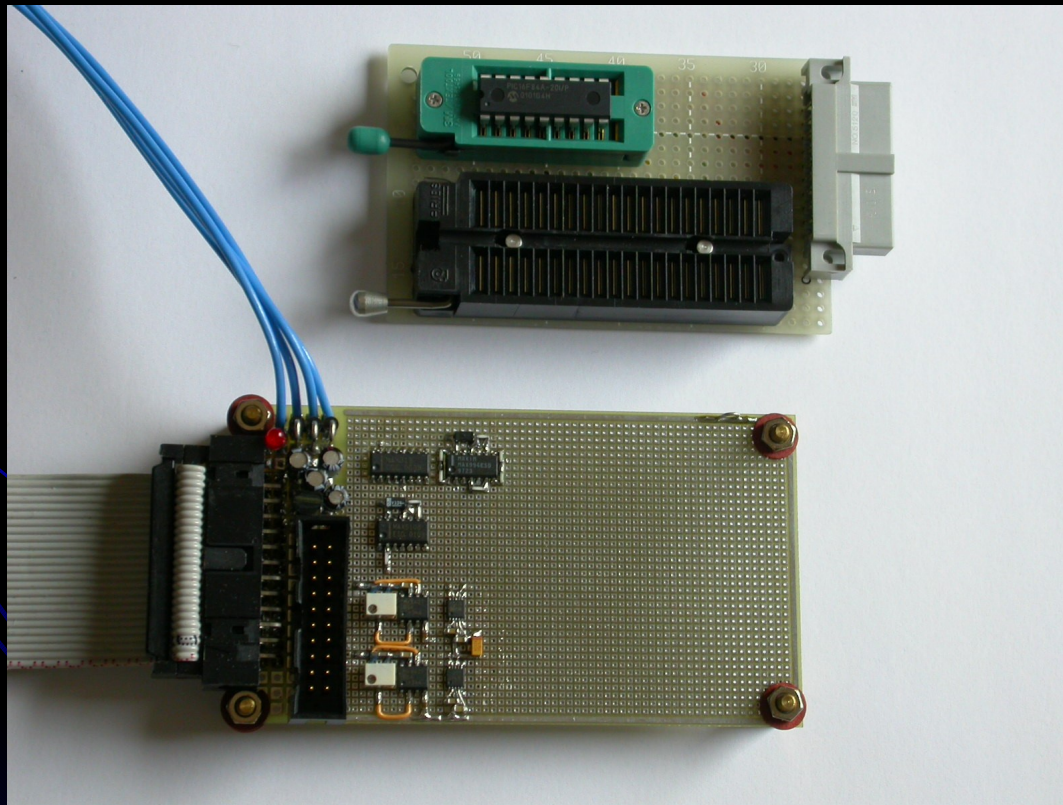
# Non-invasive attacks

- Data remanence in EEPROM and Flash
  - Memory and password/fuse are erased simultaneously
    - Fast process (difficult to control erasure)
    - $V_{TH}$  drops too low (power glitching does not work)
    - Cell charge alteration does not work
      - Voltage monitors and internally stabilized power supply
      - Internal charge pumps and timing control
      - Difficult to terminate the erase cycle



# Non-invasive attacks

- Data remanence evaluation of the Microchip PIC16F84A
  - 100  $\mu\text{V}$  precision power supply
  - 1  $\mu\text{s}$  timing control



# Non-invasive attacks

---

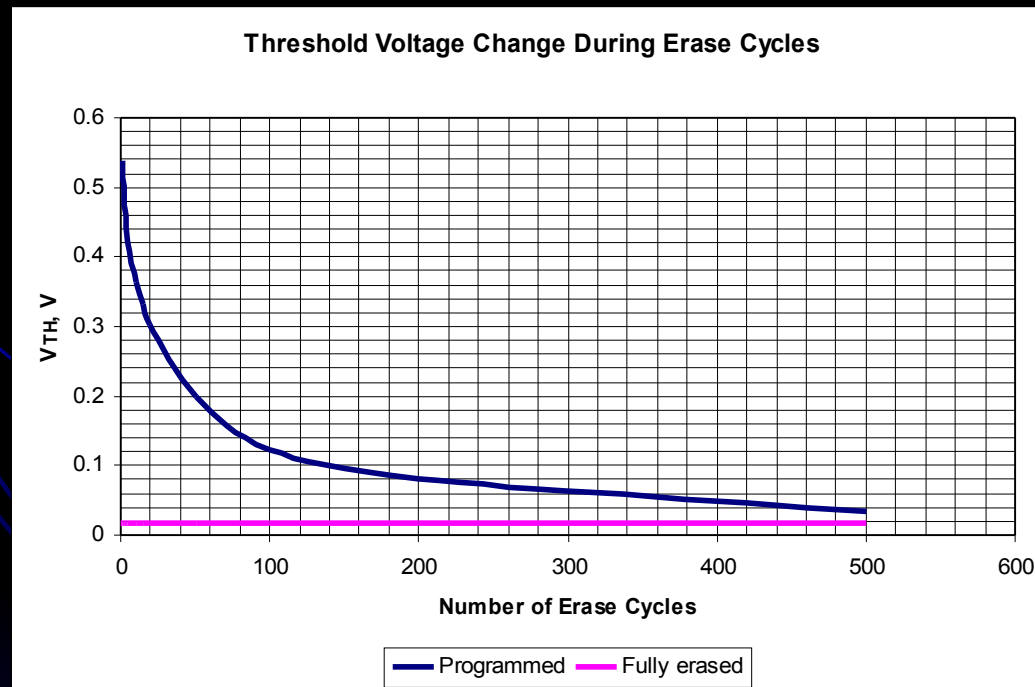
- Measuring  $V_{TH}$  close to 0 V
  - Power glitch to reduce  $V_{ref}$  to 0.5 V
    - Still not enough
  - Exploiting after-erase discharging delay
    - Accidentally discovered in year 2000
    - Shifts  $V_{TH}$  up by 0.6 ... 0.9 V
  - Applying both techniques simultaneously:
    - $V_{TH} = K V_{DD} - V_W$
    - $V_{TH} = -0.4 \dots 2.0 \text{ V}$



# Non-invasive attacks

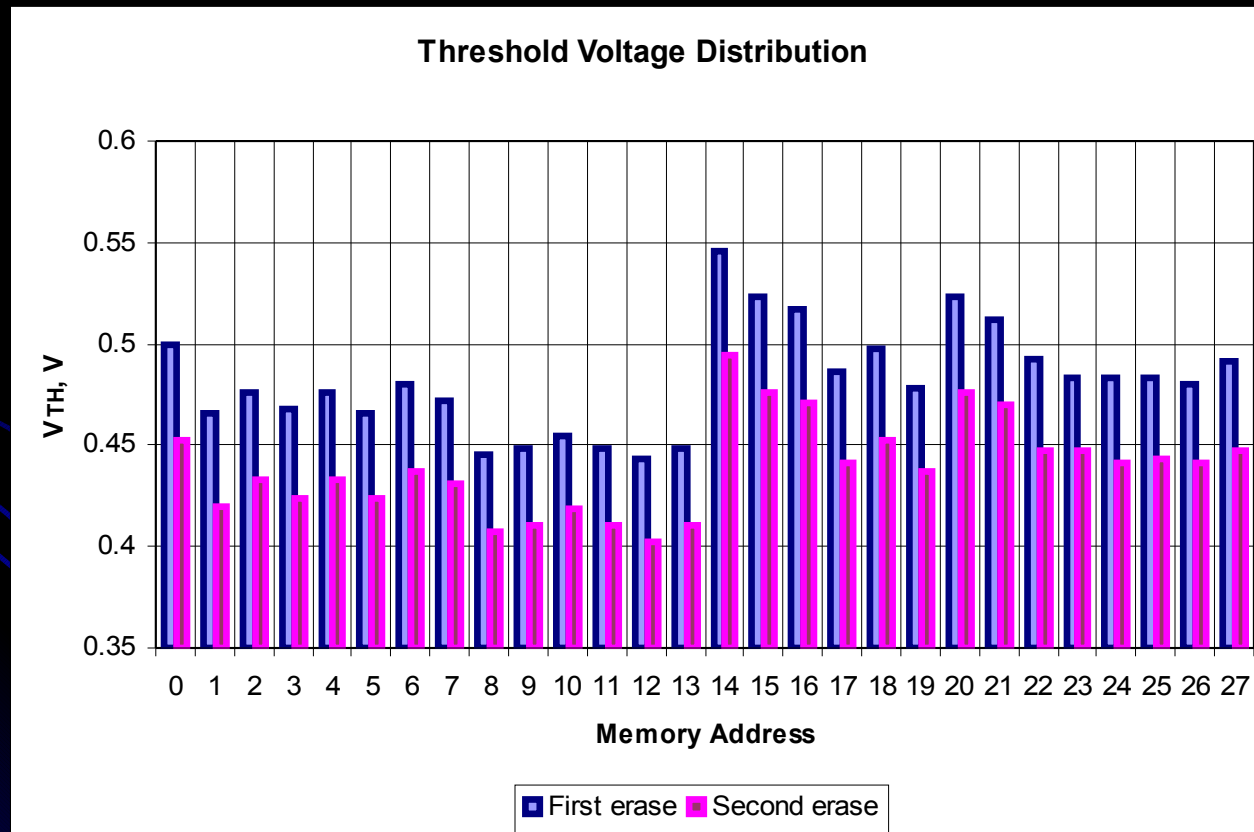
## Experimental method

- $V_{TH} = V_{ref} = K V_{DD} - V_W$ ,  $K = 0.5$ ,  $V_W = 0.7 V$
- Memory bulk erase cycles (5 V, 10 ms)
  - Flash memory, 100 cycles:  $\Delta V_{TH} = 100 mV$
  - EEPROM memory, 10 cycles:  $\Delta V_{TH} = 1 mV$



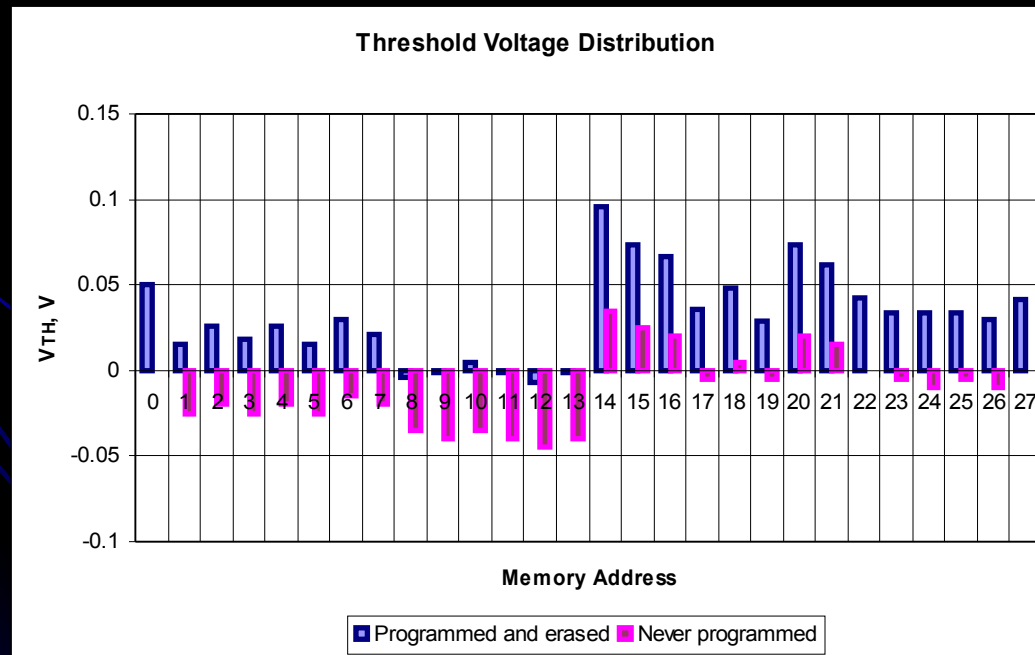
# Non-invasive attacks

- Data recovery from programmed and erased PIC16F84A
  - Large difference in  $V_{TH}$  between cells in the array
  - Measure the cell's  $V_{TH}$  before and after an extra erase cycle



# Non-invasive attacks

- Never-programmed and programmed cells
  - PIC16F84A comes programmed to all 0's
    - 10,000 erase cycles, then bake 10 h at 150°C to fully discharge cells. Measure  $V_{TH}$
    - Program to all 0's, then another 10,000 erase cycles. Measure  $V_{TH}$
  - Still noticeable change of  $\Delta V_{TH} = 40$  mV



# Invasive attacks

---

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

# Invasive attacks

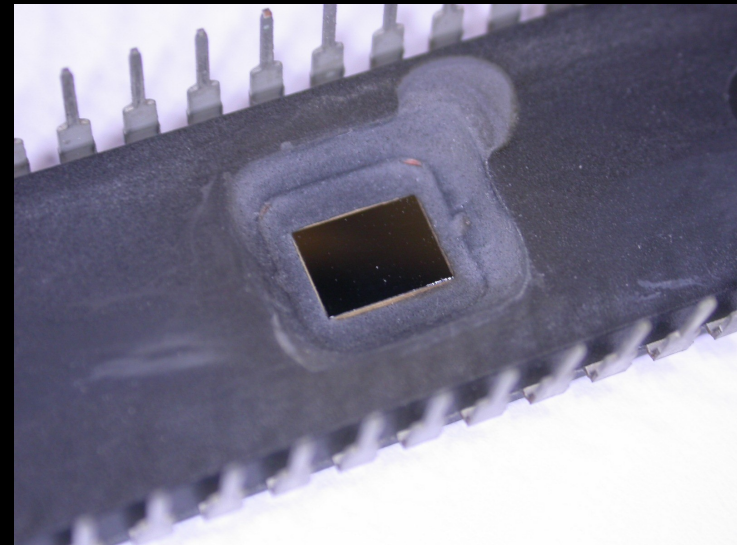
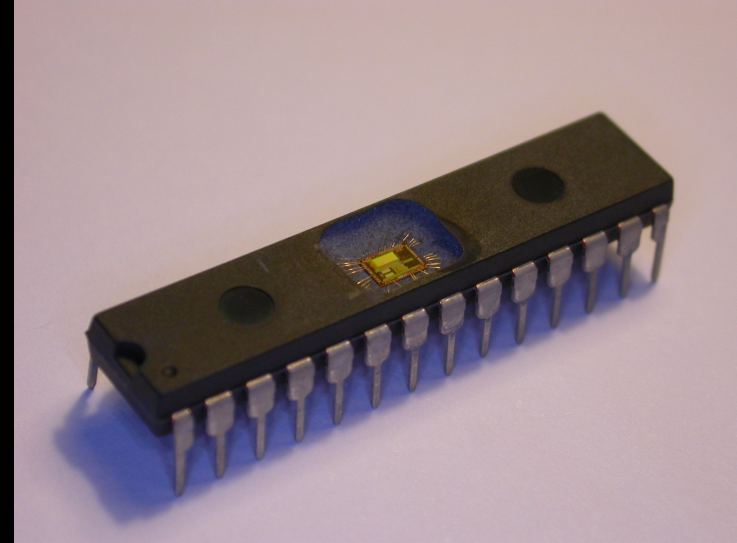
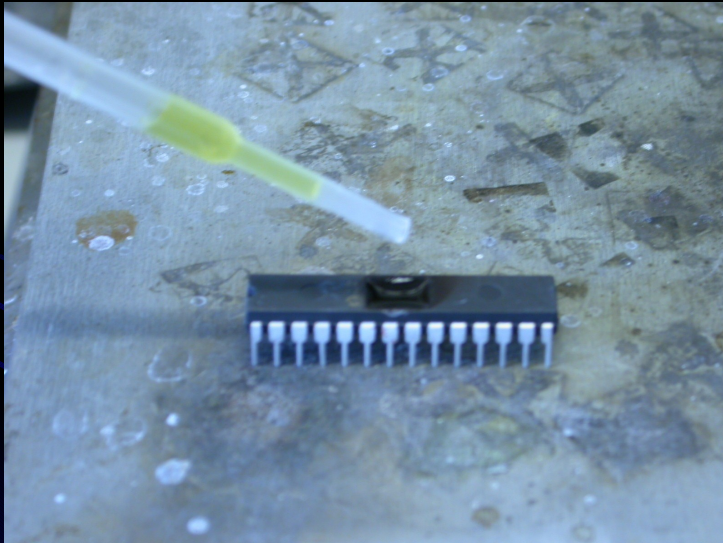
- Sample preparation
  - Decapsulation
    - Manual: using fuming nitric acid ( $\text{HNO}_3$ ) and Acetone, 60 °C
    - Automatic: using concentrated  $\text{HNO}_3$  and  $\text{H}_2\text{SO}_4$



Picture courtesy of Semiresearch Ltd

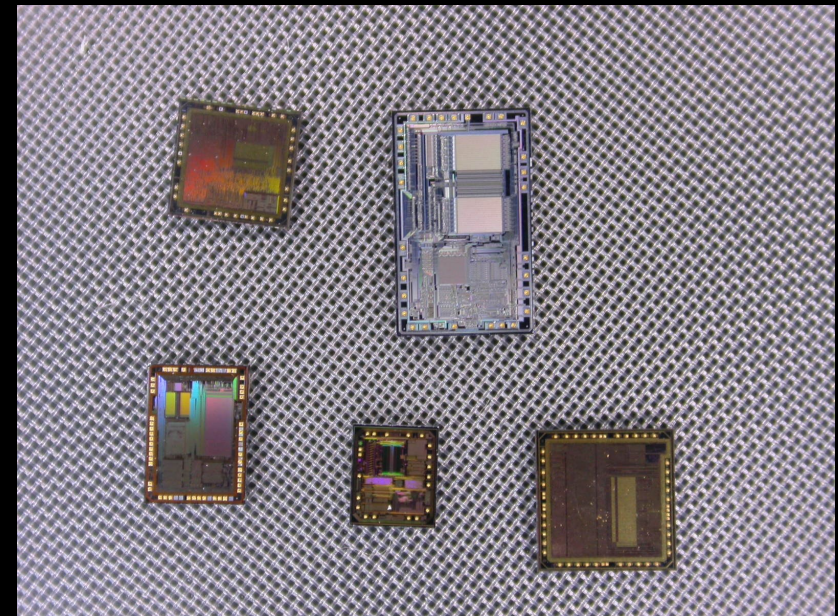
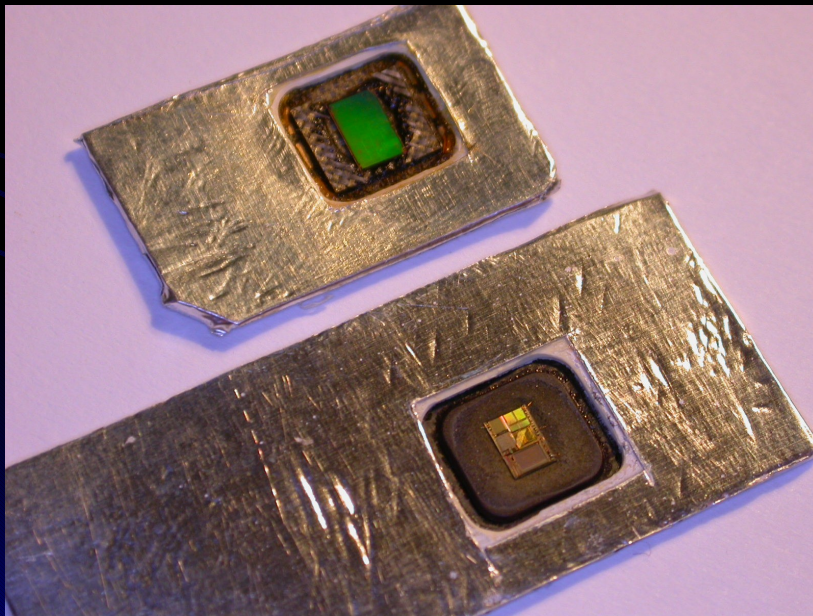
# Invasive attacks

- Sample preparation
  - Decapsulation
    - Front-side
    - Rear-side



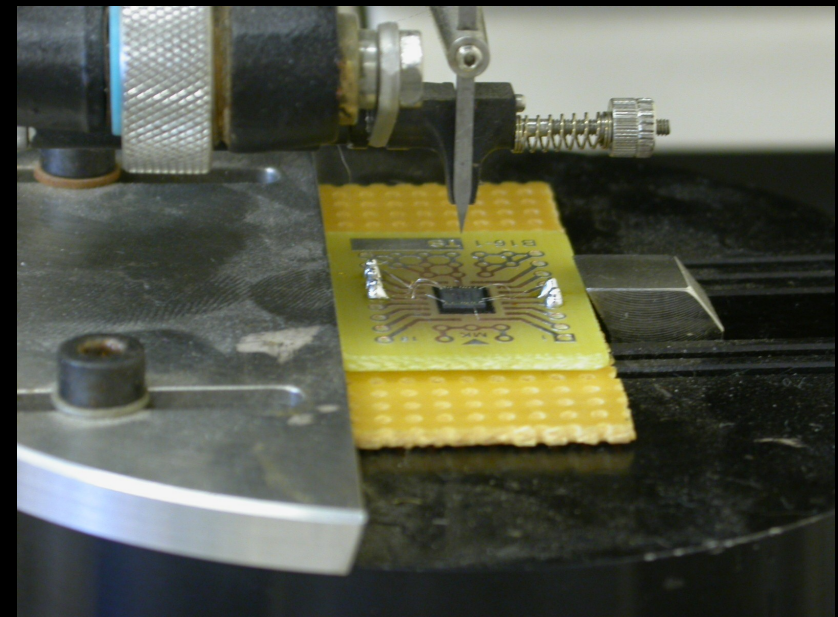
# Invasive attacks

- Sample preparation
  - Decapsulation
    - Partial
    - Full



# Invasive attacks

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

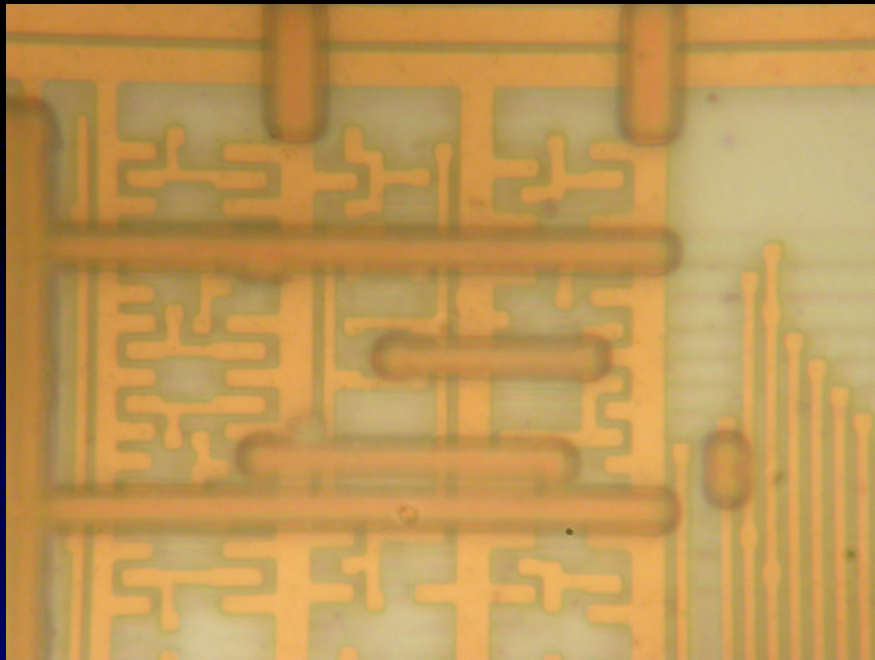




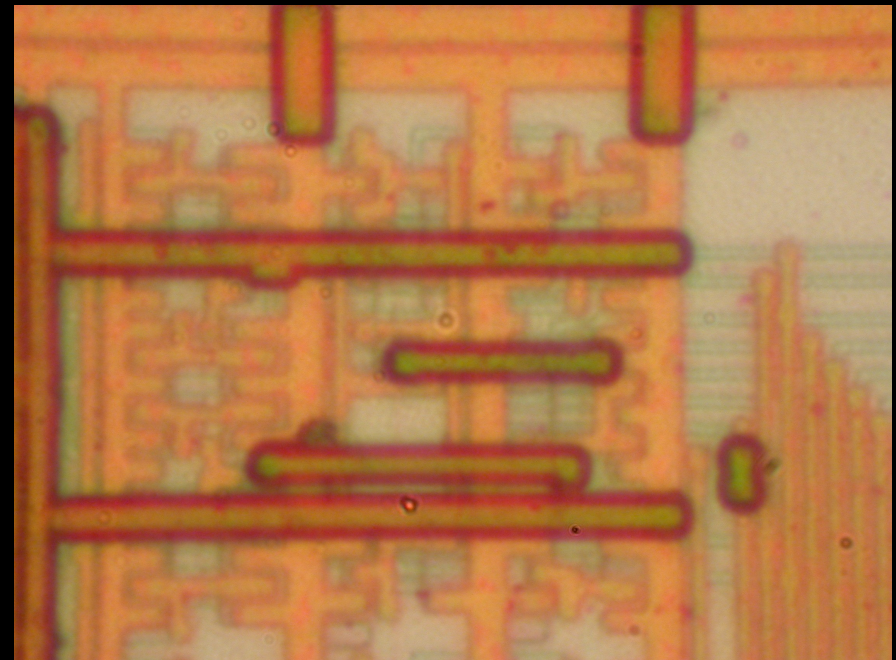
# Invasive attacks

## Optical imaging

- Resolution is limited by optics and wavelength of a light
  - $R = 0.61 \lambda / NA = 0.61 \lambda / n \sin(\mu)$ 
    - 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  $NA = 0.95$ )



Leitz Ergolux AMC, 100 $\times$ , NA = 0.9

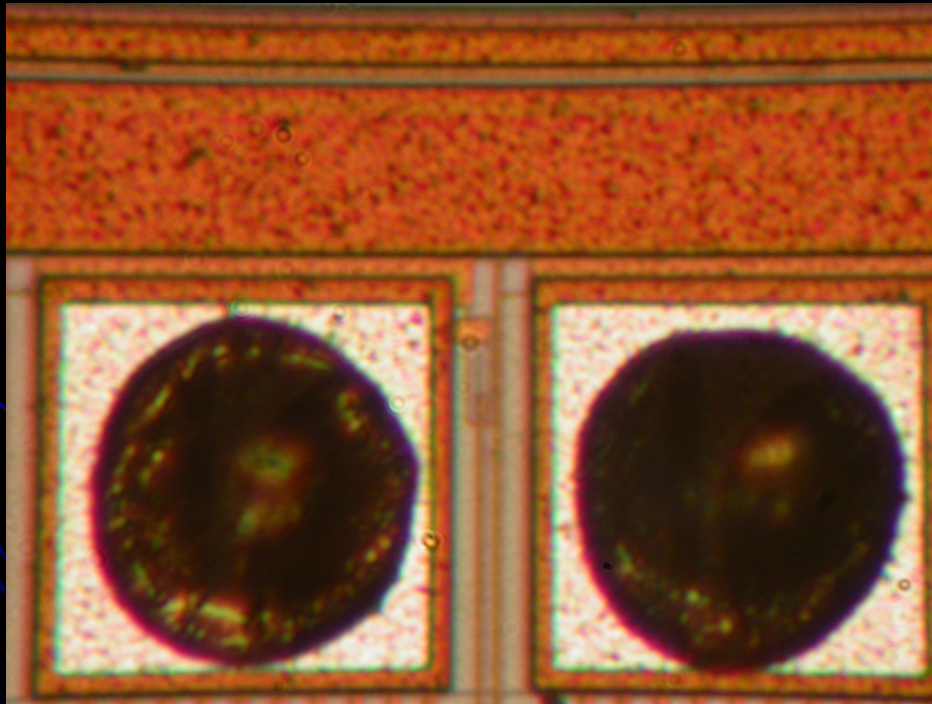


Bausch&Lomb MicroZoom, 50 $\times$ 2 $\times$ , NA = 0.45

# Invasive attacks

---

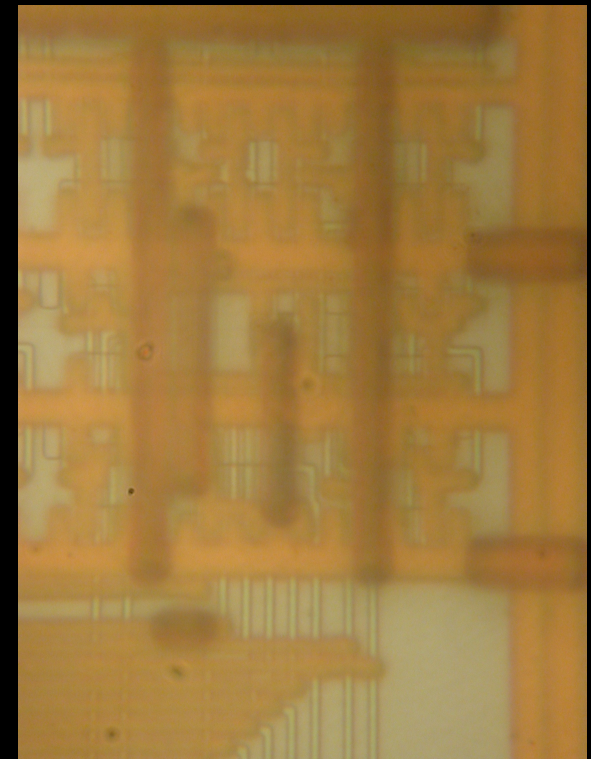
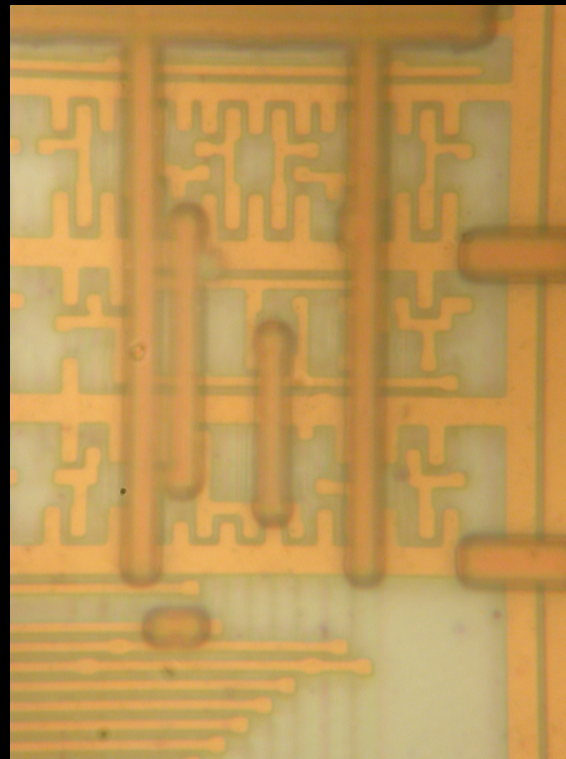
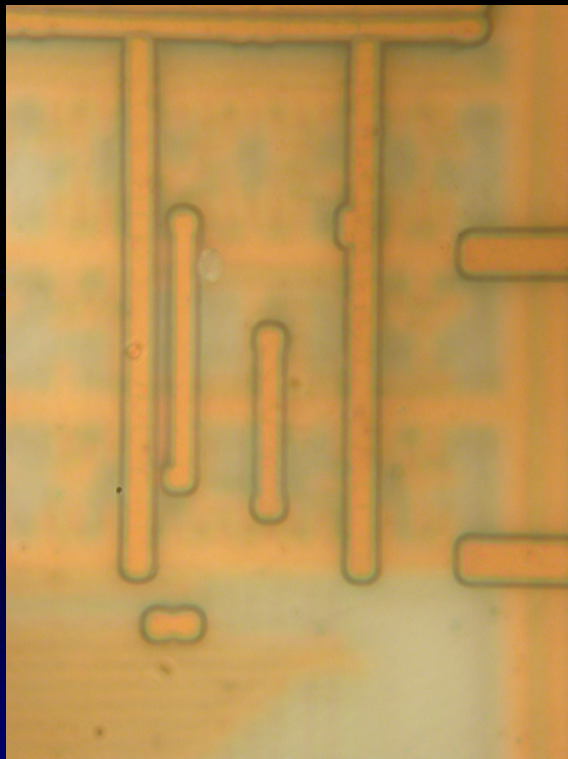
- **Optical imaging**
  - Image quality depends on microscope optics
    - Colour aberrations and geometric distortions
      - Reduce resolution
      - Problems with merging images



# Invasive attacks

---

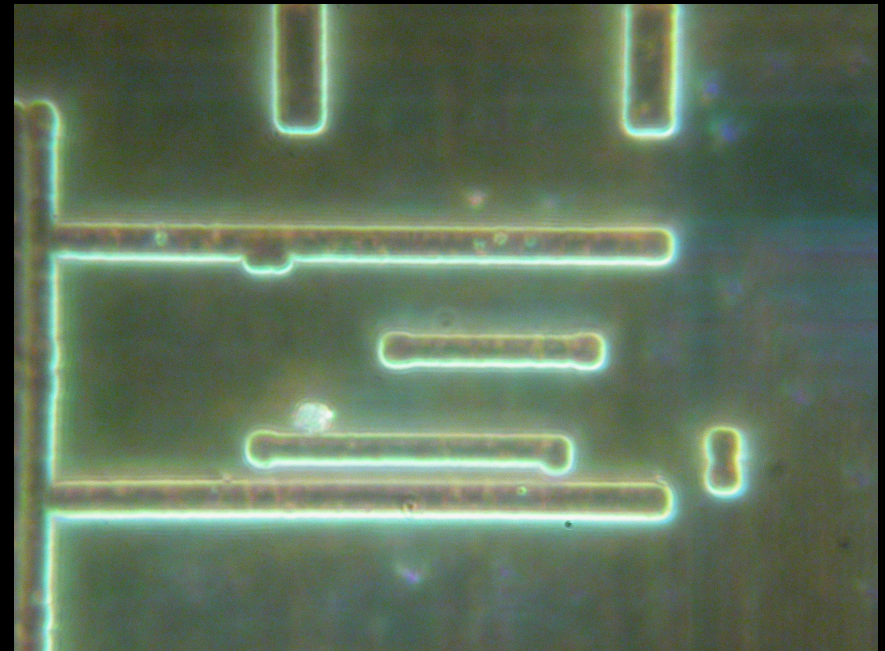
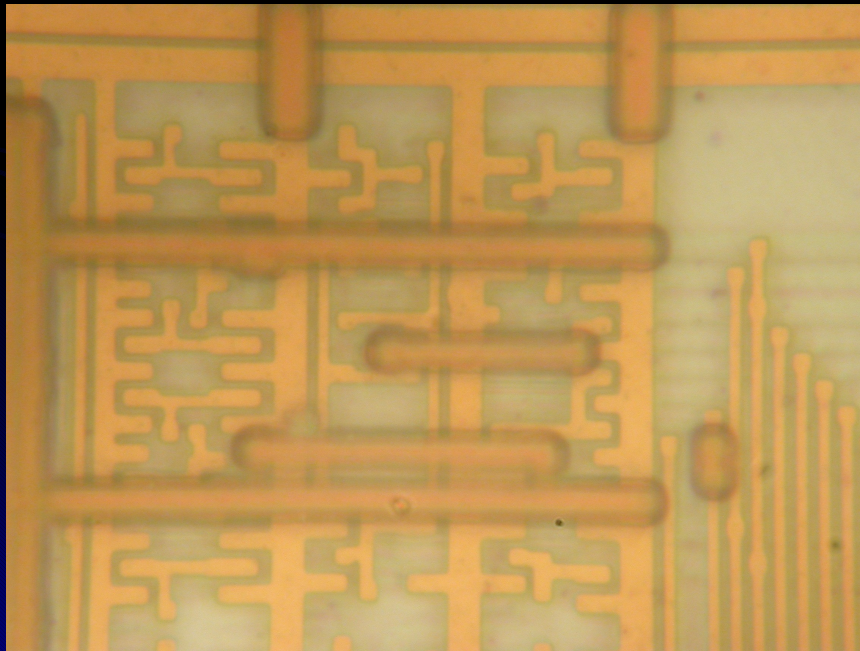
- Optical imaging
  - Image quality depends on microscope optics
    - Depth of focus



# Invasive attacks

---

- Optical imaging
  - Additional features aimed at increasing resolution and contrast
    - Darkfield illumination (only edges are visible)
    - Polarising contrast (reduces reflections)
    - Confocal imaging (separates layers)



# 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
    - Isotropic – uniformity in all directions
    - Uneven etching and undercuts (metal wires lift off the surface)
  - Plasma etching (dry etching)
    - Perpendicular to the surface
    - Speed varies for different materials
  - Chemical-mechanical polishing
    - Good planarity and depth control, suitable for modern technologies
    - Difficult to maintain planarity of the surface, special tools required

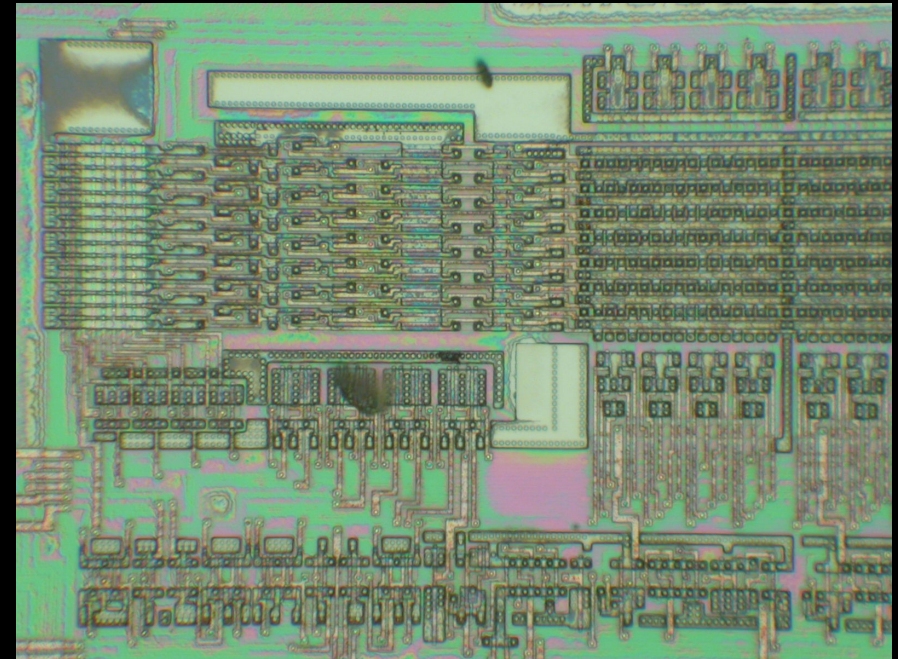
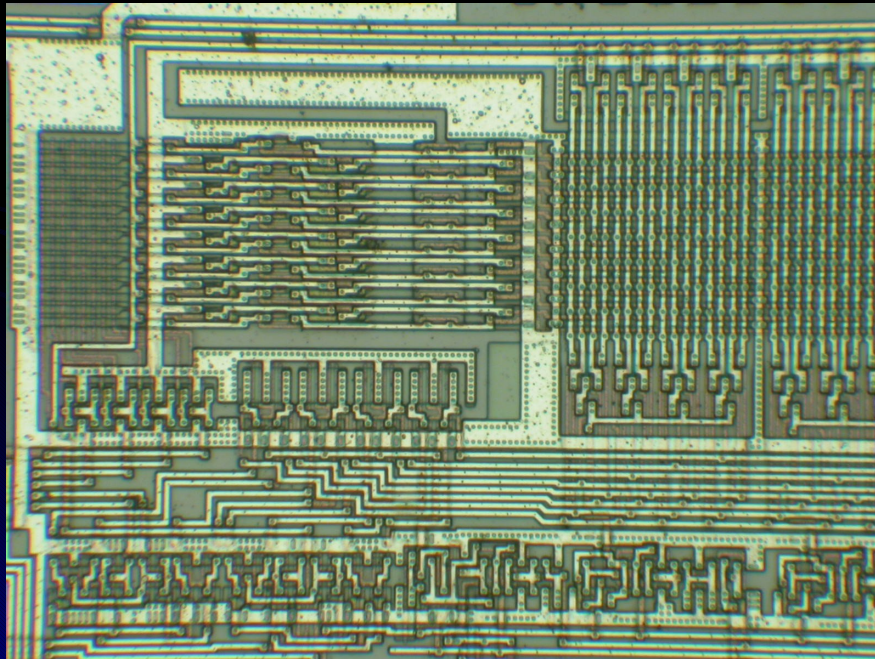
# Invasive attacks

- Deprocessing
  - Wet chemical etching
    - Hydrofluoric acid or fluoride-ion solutions for passivation and  $\text{SiO}_2$
    - KOH solutions, HCl or  $\text{H}_2\text{O}_2$  for silicon and metals
  - Dry plasma etching
    - $\text{CF}_4$ ,  $\text{C}_2\text{F}_6$ ,  $\text{SF}_6$  or  $\text{CCl}_4$  gases



# Invasive attacks

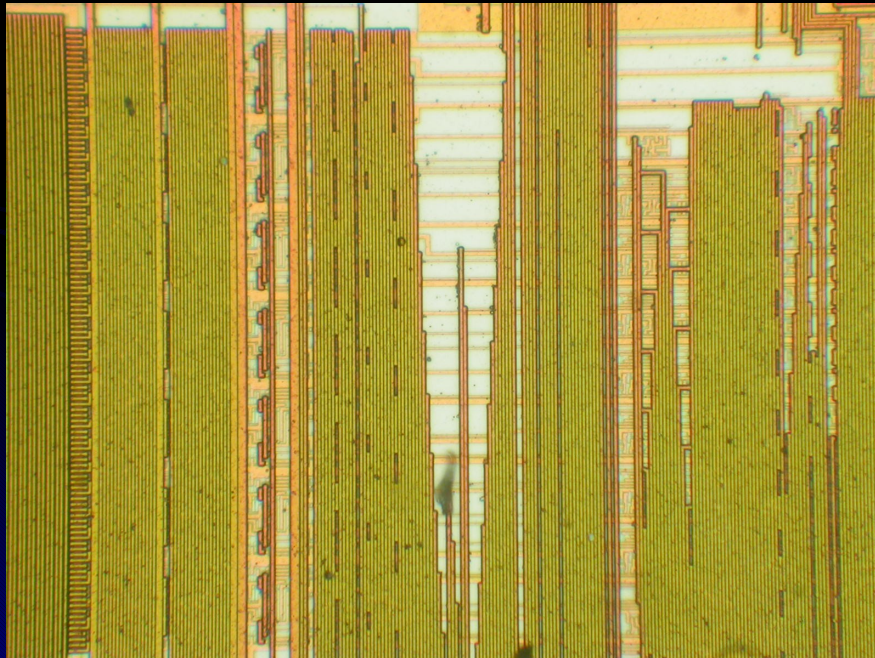
- Removing top metal layer using wet chemical etching
  - Good uniformity over the surface
  - Works reliably only for chips fabricated with  $0.8\ \mu\text{m}$  or larger technology (without polishing layers)



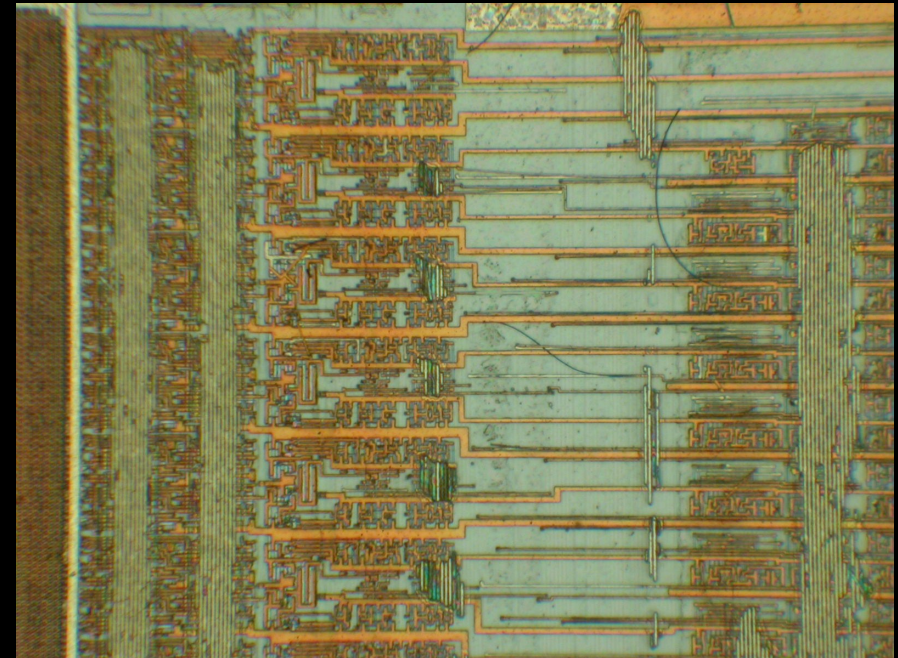
Motorola MC68HC705C9A microcontroller

# Invasive attacks

- Removing top metal layer using wet chemical etching
  - Unsuitable for chip fabricated with  $0.5\ \mu\text{m}$  or smaller technology (with chemical-mechanical polishing) because of undercuts, under- and over-etching



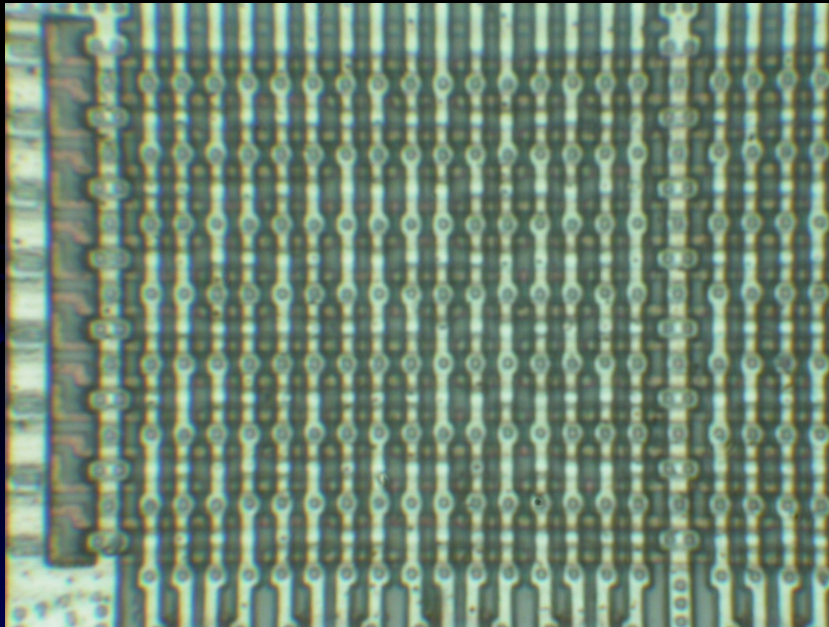
Microchip PIC16F76 microcontroller



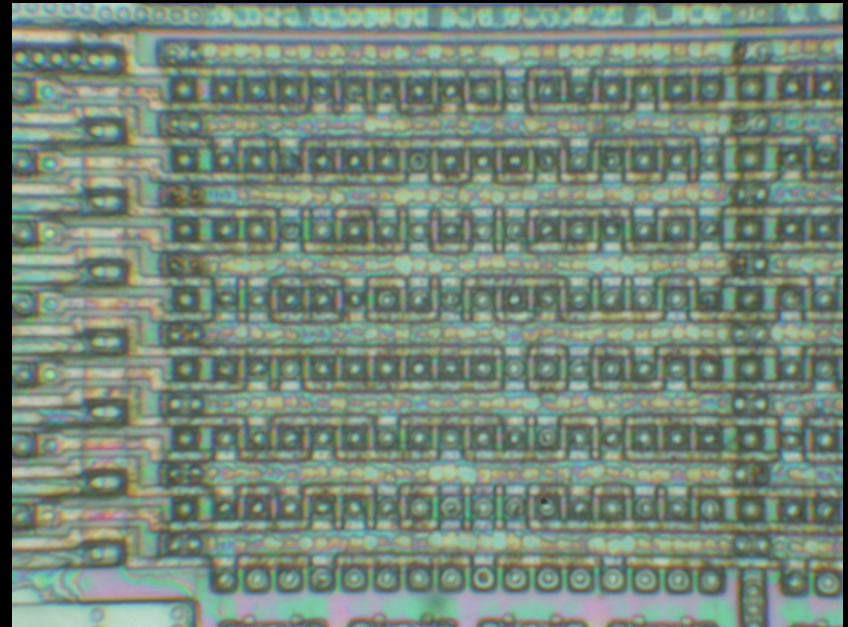


# Invasive attacks

- 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 implantation) used in smartcards

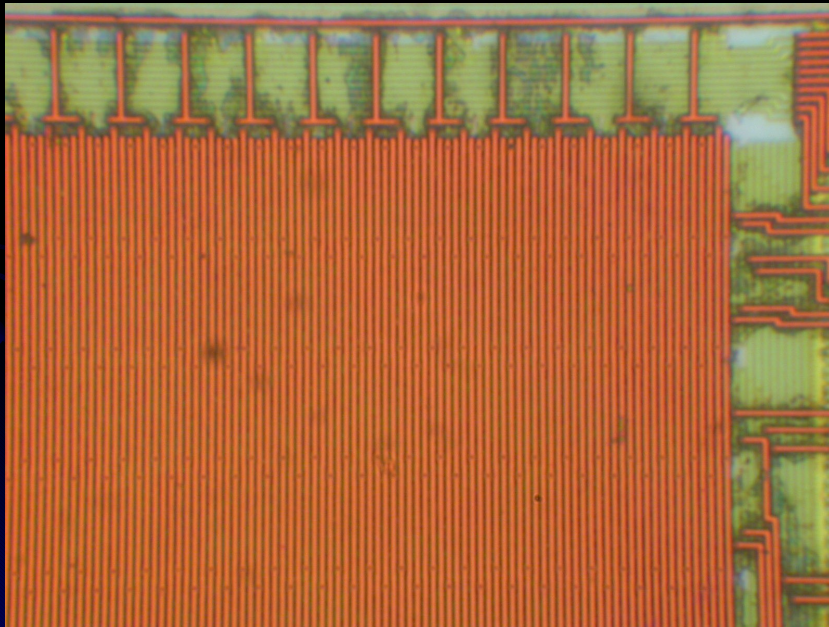


Motorola MC68HC705P6A microcontroller

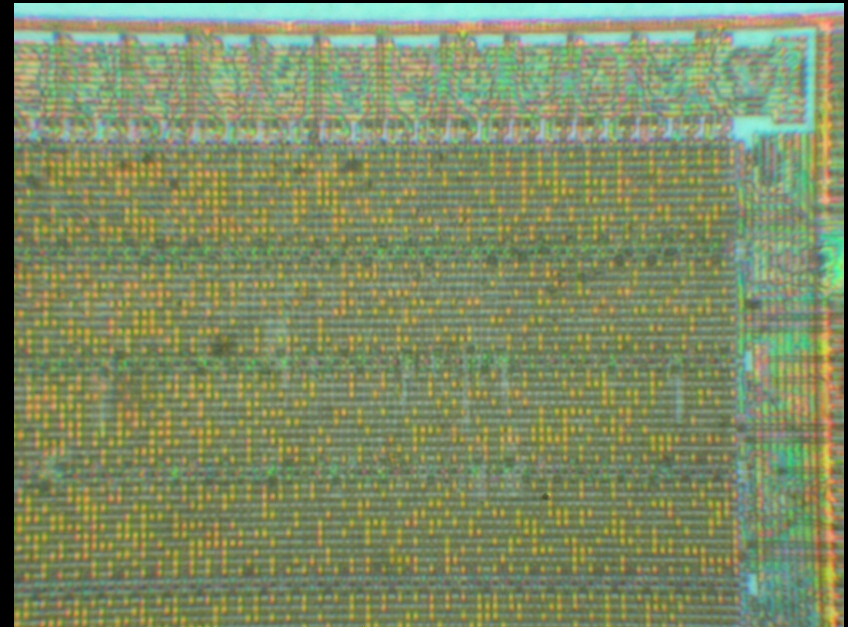


# Invasive attacks

- Memory extraction from Mask ROMs
  - Selective etching of metal layers for direct optical observation of data in NOR ROMs (bits programmed by contact layer)
  - Not suitable for VTROM (ion implantation) used in smartcards



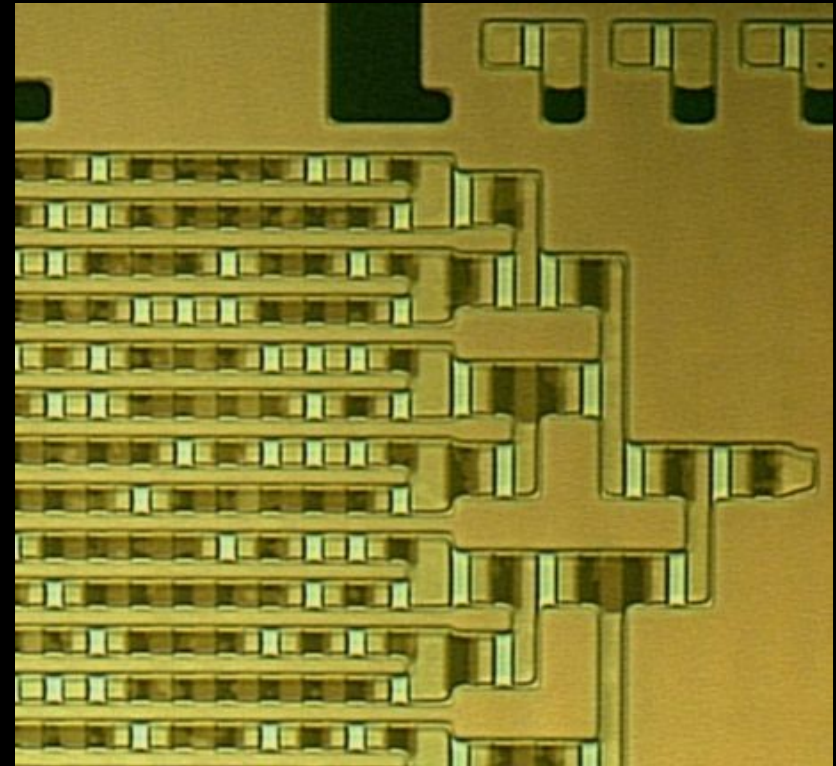
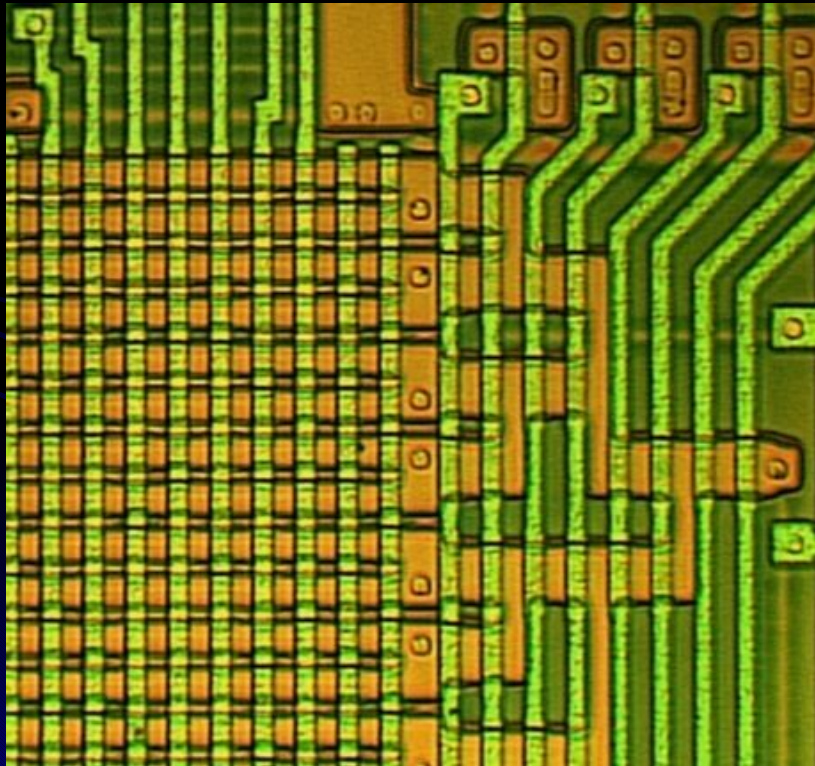
NEC  $\mu$ PD78F9116 microcontroller



# Invasive attacks

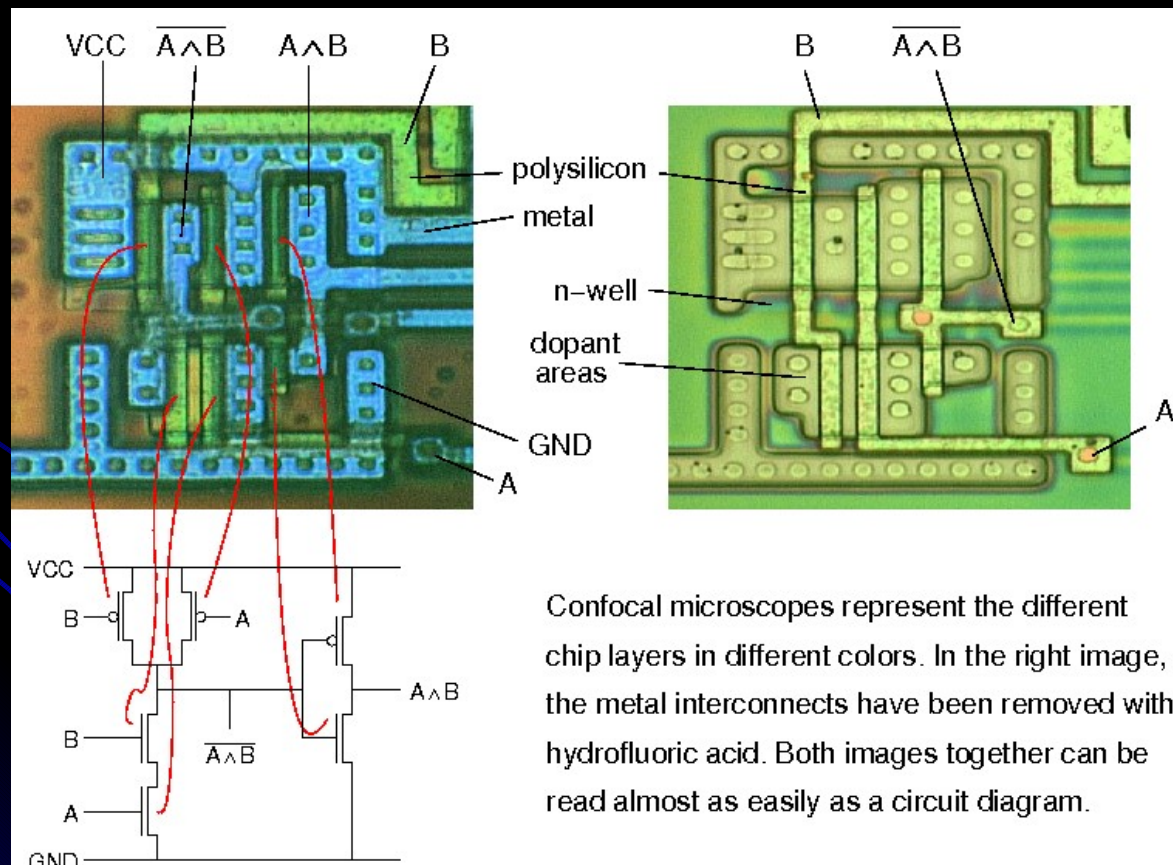
- Memory extraction from Mask ROMs
  - Selective (dash) etchants reacts with doped and non-doped regions at different speeds, exposing the ROM bits

O. Kömmerling M. Kuhn, 1999



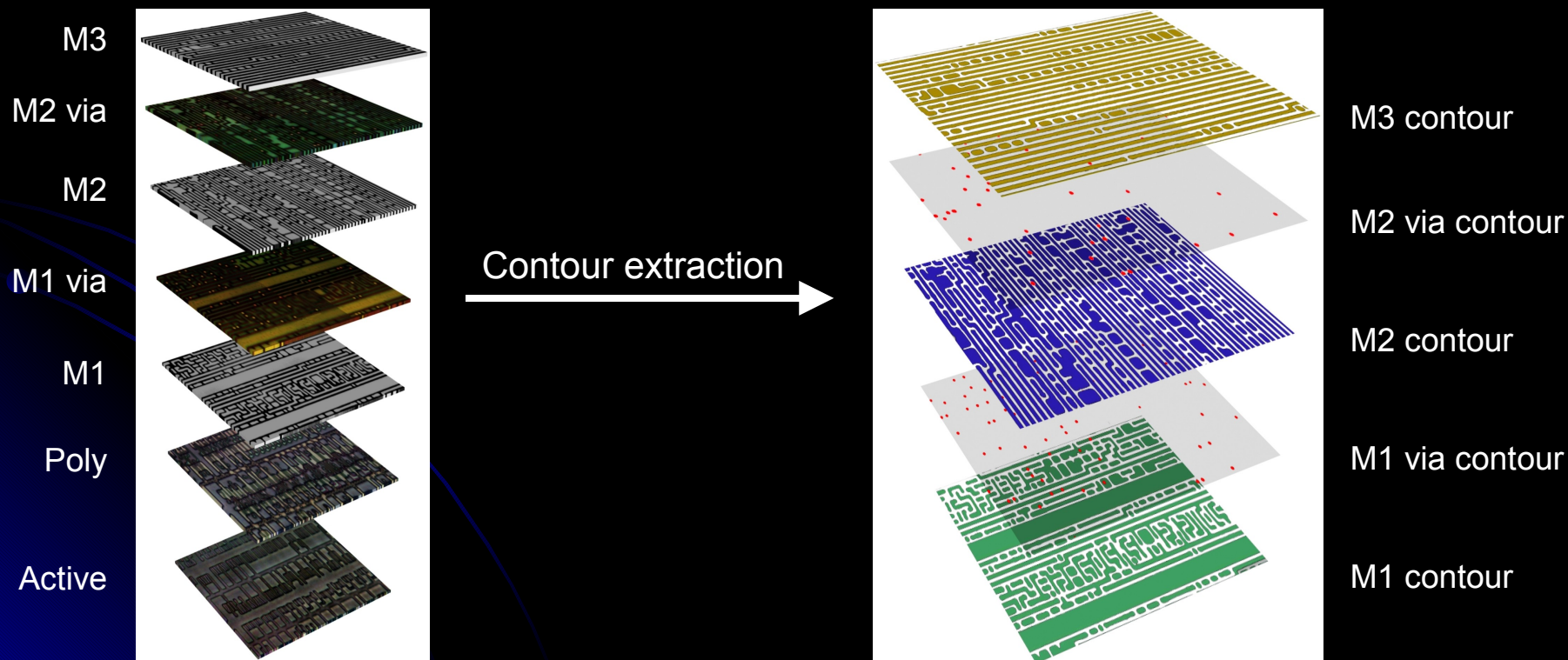
# Invasive attacks

- Reverse engineering – understanding the structure of a semiconductor device and its functions
  - Optical – using a confocal microscope (for  $> 0.5 \mu\text{m}$  chips)



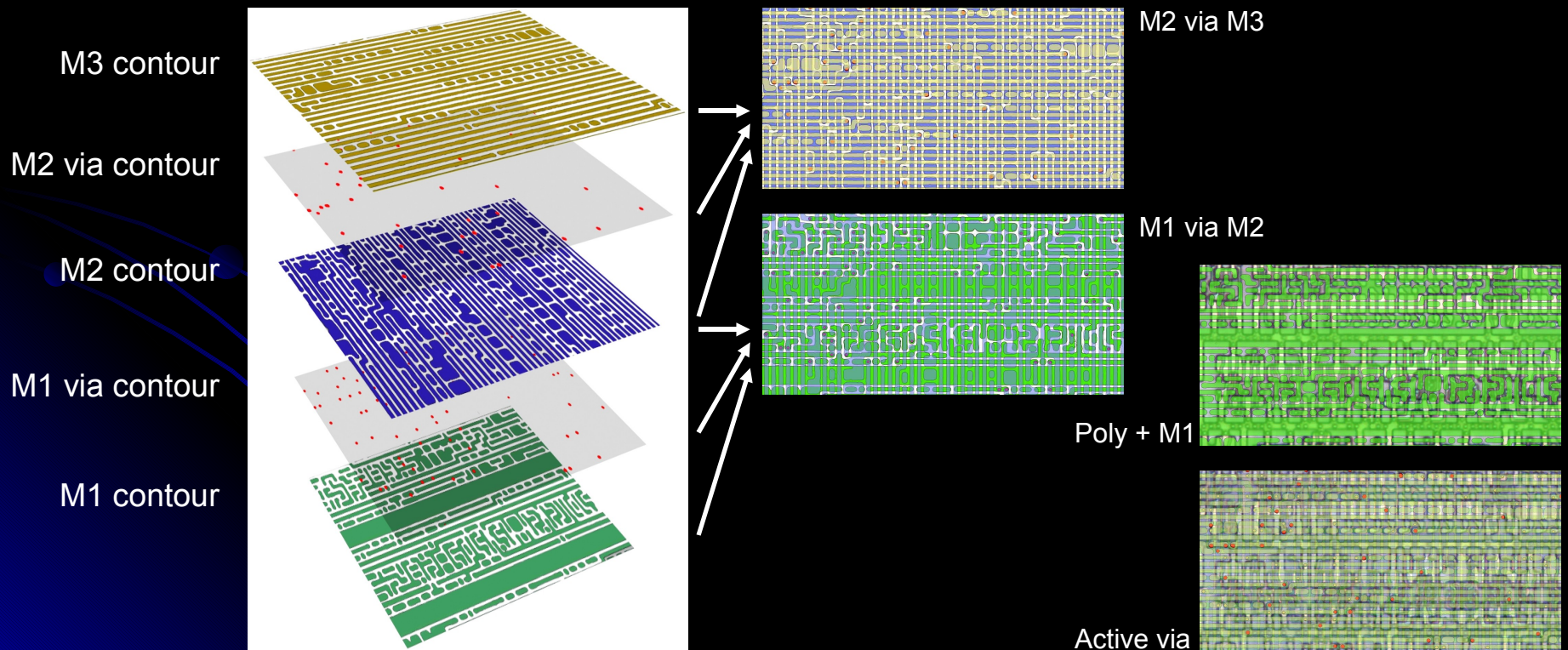
# Invasive attacks

- Reverse engineering of modern deep-submicron chips
  - Decomposition using plasma-chemical etching and polishing
  - Taking high-resolution digital images (SEM for  $<0.18 \mu\text{m}$  chips)
  - Merging digital images creating a large image of the surface



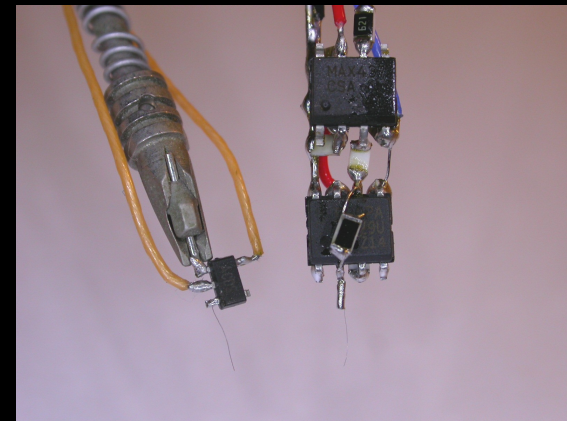
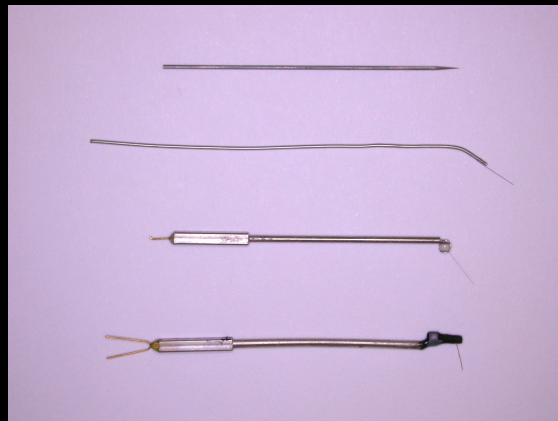
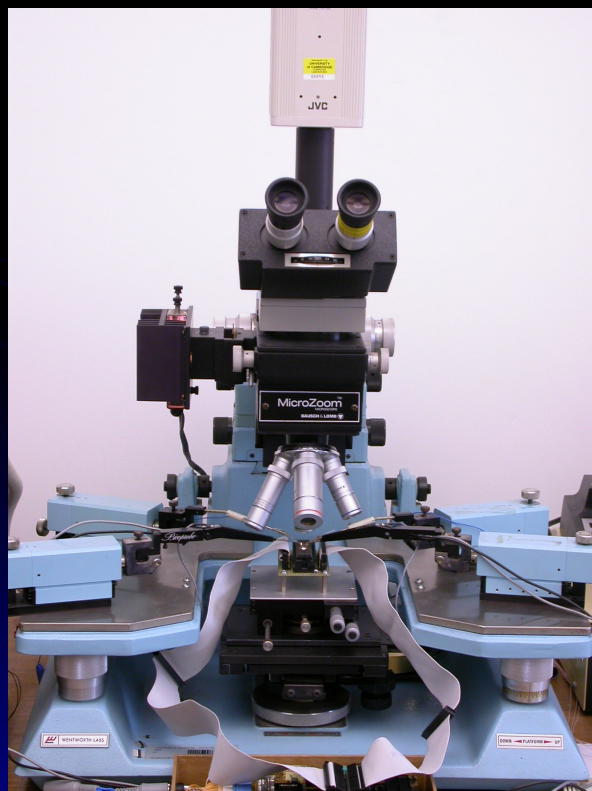
# Invasive attacks

- Reverse engineering of modern deep-submicron chips
  - Aligning and stitching images together creating layer pairs
  - Netlist extraction creating a gate-level circuit diagram
  - Converting the Netlist into VHDL file for simulation and analysis



# Invasive attacks

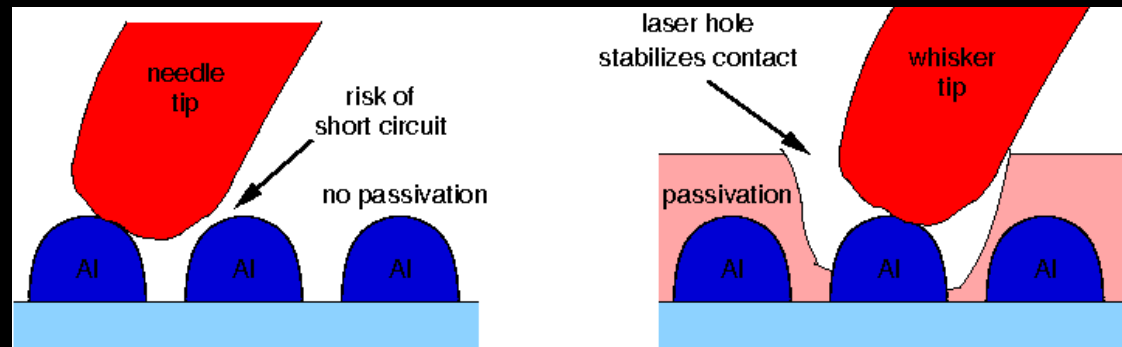
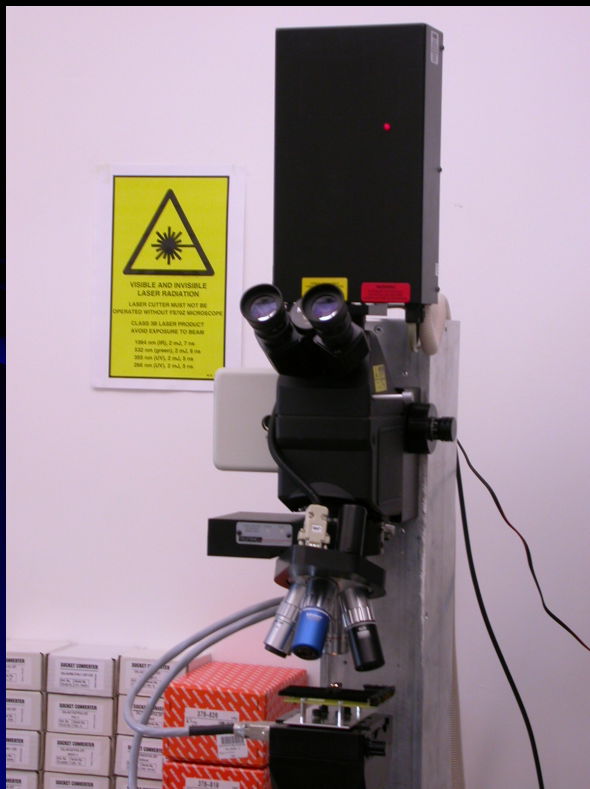
- Microprobing with fine electrodes
  - Eavesdropping on signals inside a chip
  - Injection of test signals and observing the reaction
  - Used for extraction of secret keys and memory contents



# 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



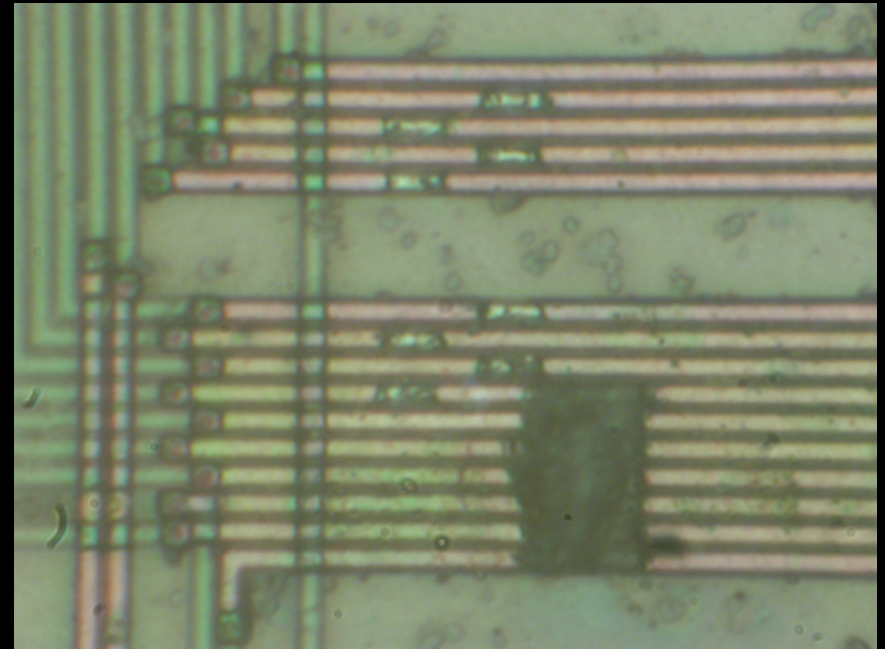
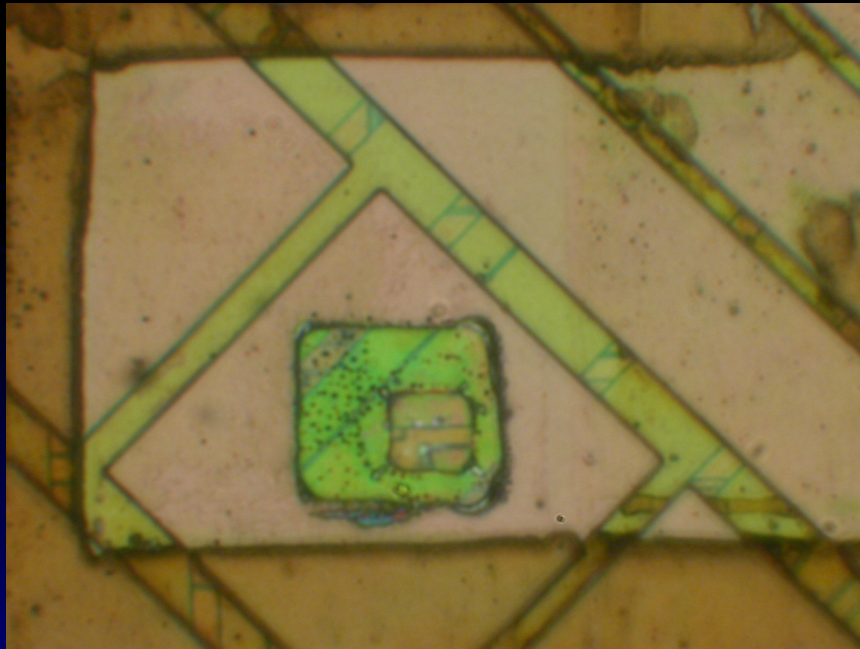
Picture courtesy of Dr Markus Kuhn



# Invasive attacks

---

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

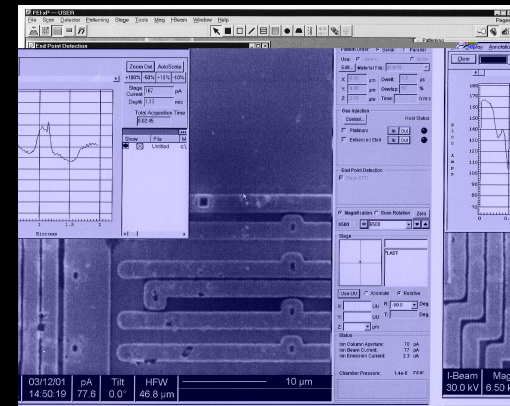


# Invasive attacks

- Focused Ion Beam workstation
  - Chip-level surgery with 10 nm precision
  - Etching with high aspect ratio
  - Platinum and  $\text{SiO}_2$  deposition



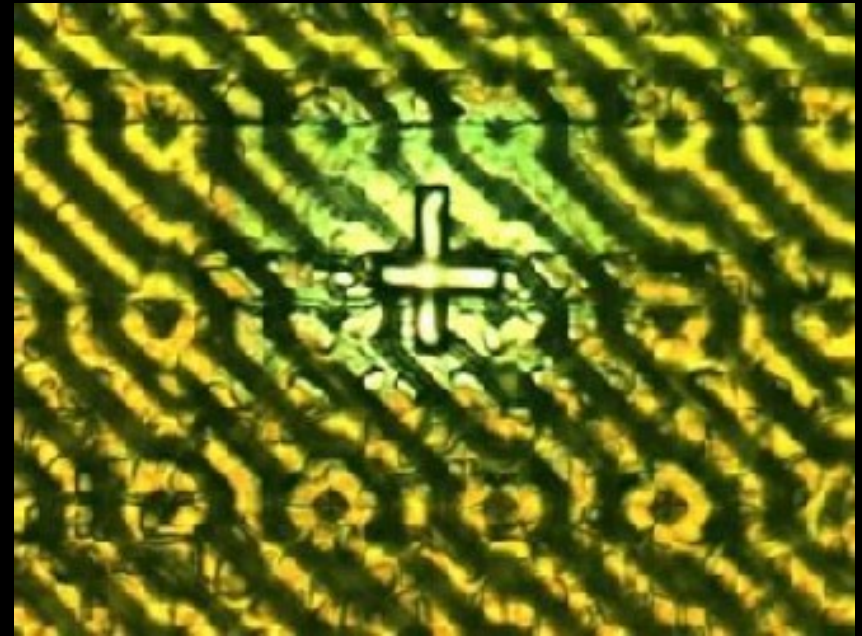
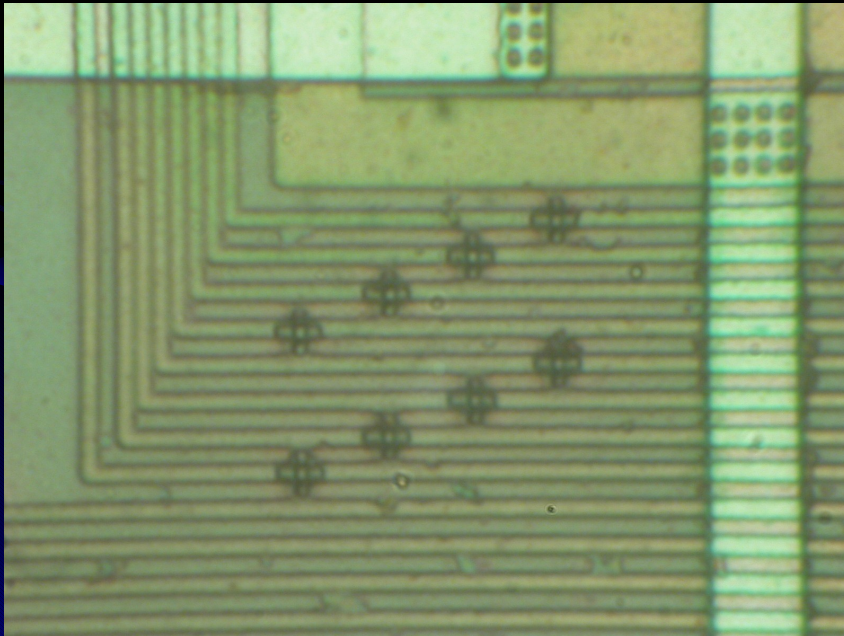
Picture courtesy of Semiresearch Ltd



# 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  $\mu\text{m}$

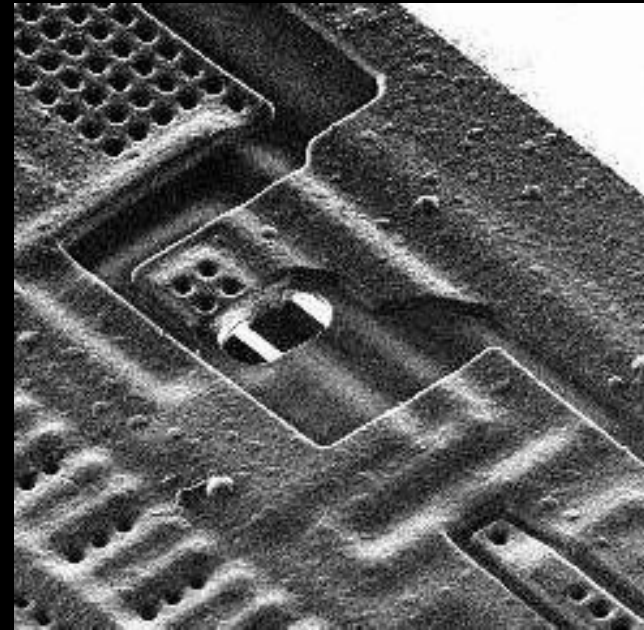
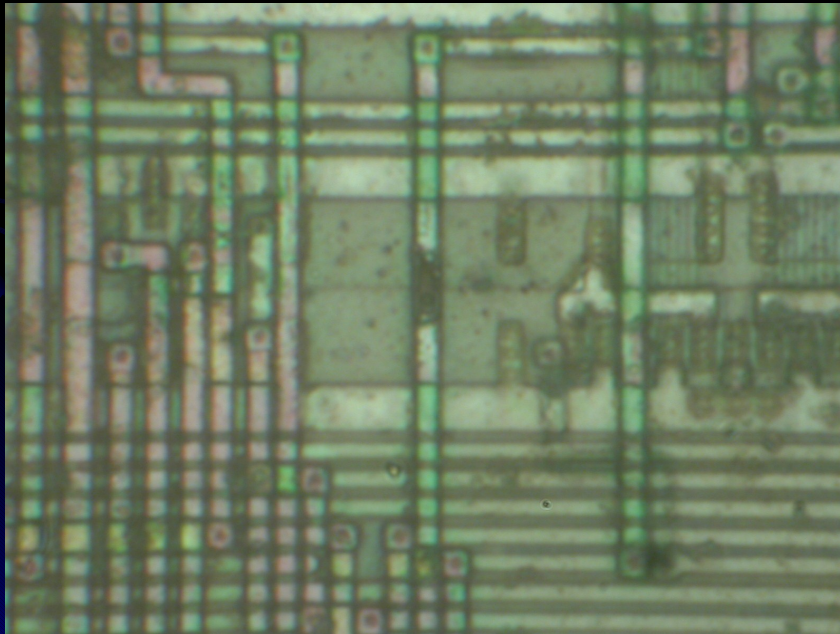


Picture: Oliver Kömmerling

# Invasive attacks

---

- Chip modification
  - Cutting a wire from the security-fuse sensor circuit
  - Restoring the blown security fuse

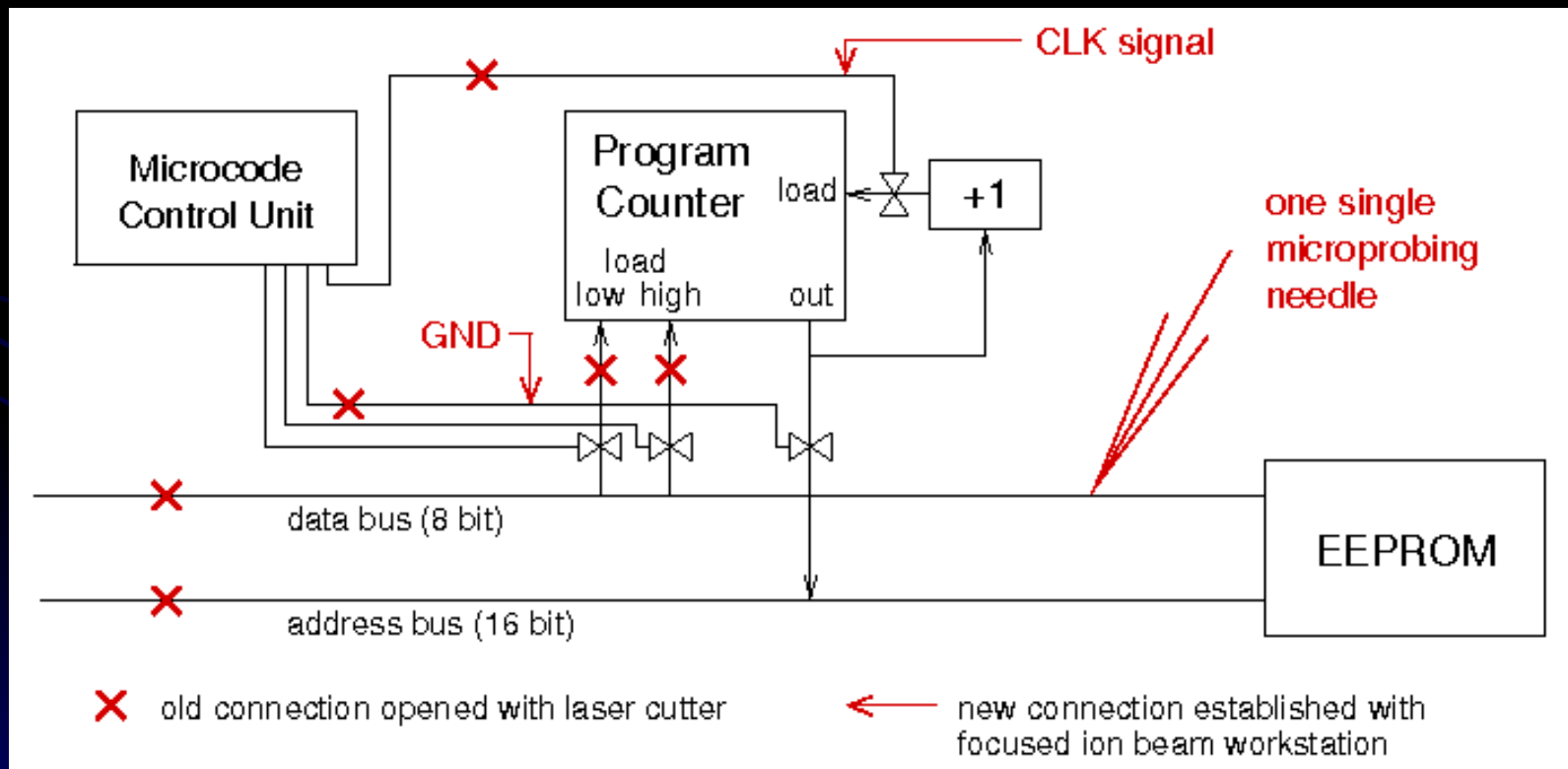


Picture: Oliver Kömmerling

# 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



# Semi-invasive attacks

---

- Filling the gap between non-invasive and invasive attacks
  - Less dangerous 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 analyzer and oscilloscope
  - High-resolution optical microscope
  - Special microscopes (laser scanning, infrared etc.)
  - UV light sources
  - Heating tools
  - X-ray sources
  - Scanning electron microscope
  - PC with data acquisition board or FPGA prototyping boards

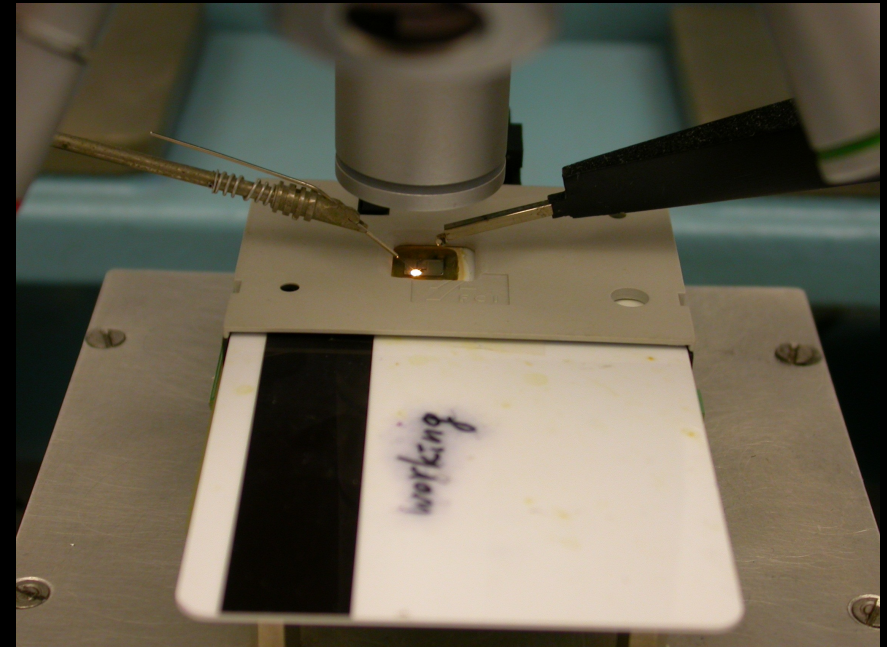
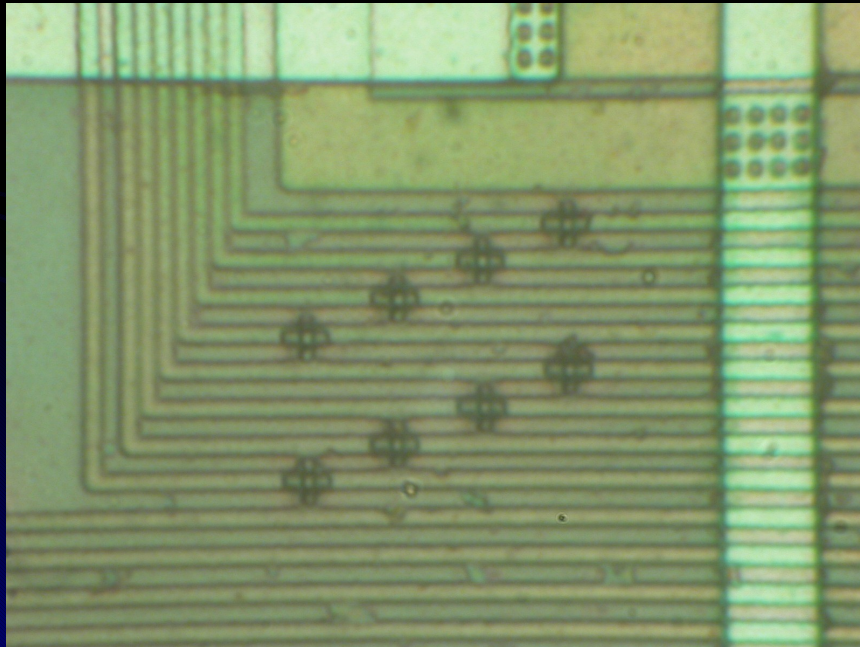
# Semi-invasive attacks

---

- 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

- History of semi-invasive attacks
  - Optical fault injection was observed in my experiments with microprobing attacks in early 2001





# Semi-invasive attacks

- Sample preparation
  - Decapsulation techniques (manual or automatic by using  $\text{HNO}_3$ )
  - Scanning Acoustic Tomography (Hitachi MI-SCOPE 10)
    - Analysis of the inner IC package content



# Semi-invasive attacks

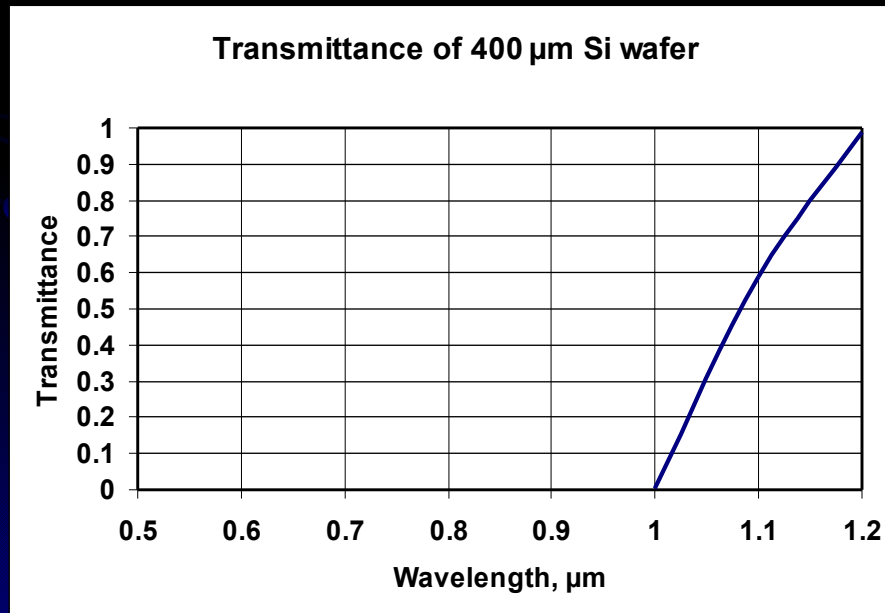
---

## ■ UV attacks

- Well known for over 20 years and used for EPROM and EEPROM
- Usually do not work on chips fabricated with 0.35  $\mu\text{m}$  or smaller process
  - Multiple metal layers block >95% of the active area
  - CMP process used in fabrication of modern chips diffuse the light
- Not suitable for most Flash devices
  - Do not affect the charge on the floating gate
  - Damages the device by shifting transistor's  $V_{\text{TH}}$  into abnormal state
- Most of modern microcontrollers have protection against UV attacks
  - Top metal protection layers
  - UV detectors using same type of cells
  - Inverted cells (UV changes the state from erased to programmed)
  - Self-destructors (UV sensitive reference cells)

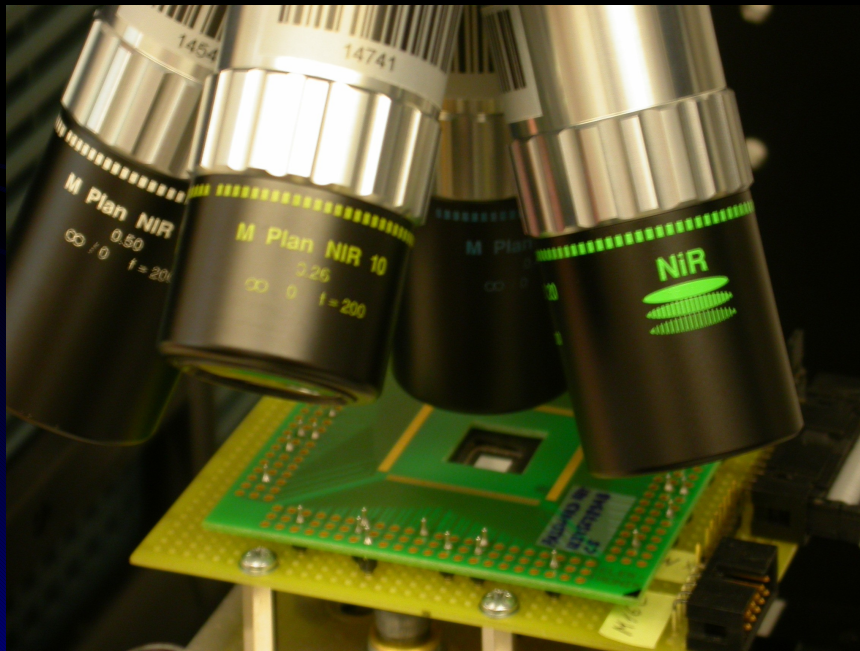
# Semi-invasive attacks

- Advanced imaging techniques
  - Approaching chip from rear side with infrared light
  - Silicon is almost transparent to photons with  $\lambda > 1100$  nm



# Semi-invasive attacks

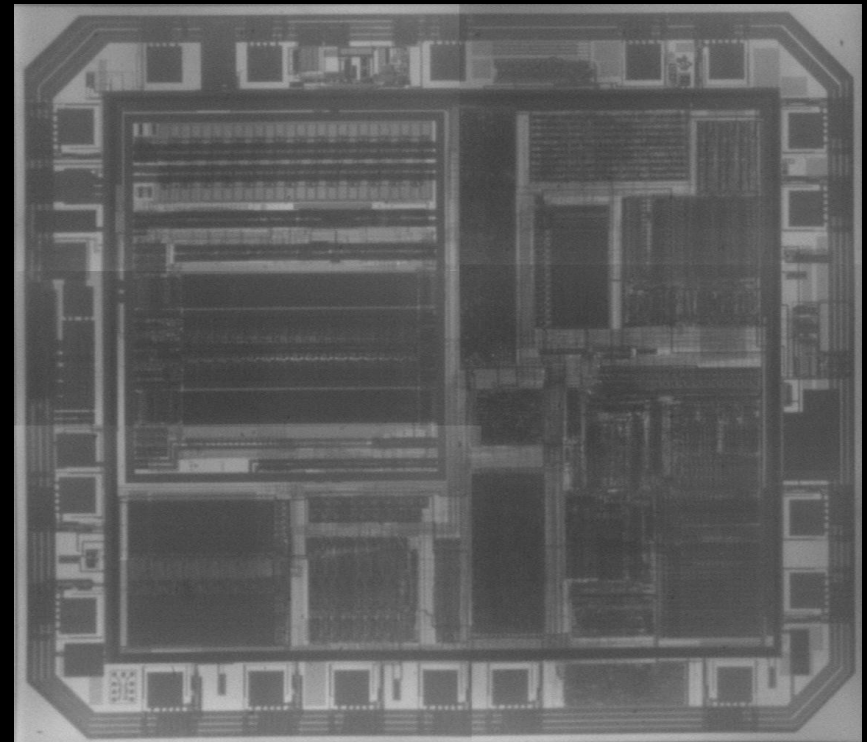
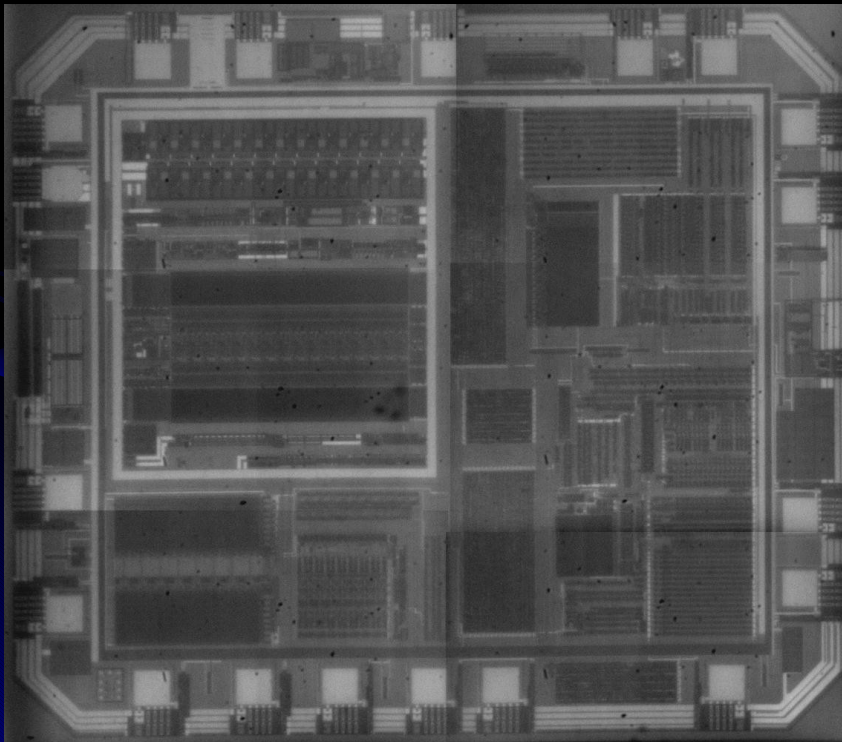
- Backside infrared imaging
  - Microscopes with IR optics should be used
  - IR enhanced CCD cameras or special cameras must be used
  - Resolution is limited to  $0.6 \mu\text{m}$  by the wavelength of used light



# Semi-invasive attacks

---

- Backside infrared imaging
  - Reflected and transmitted light illumination can be used

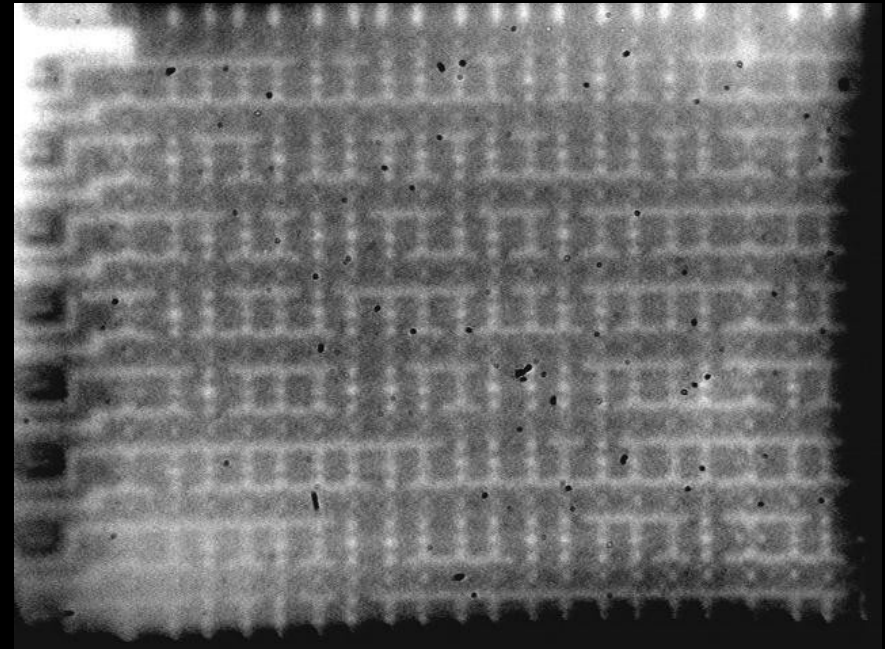
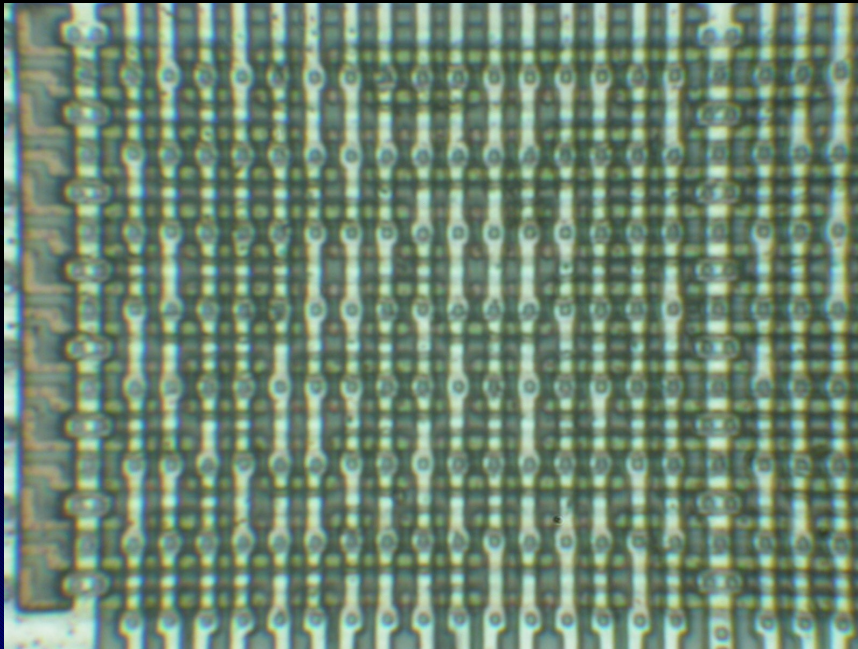


Texas Instruments MSP430F112 microcontroller

# Semi-invasive attacks

---

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

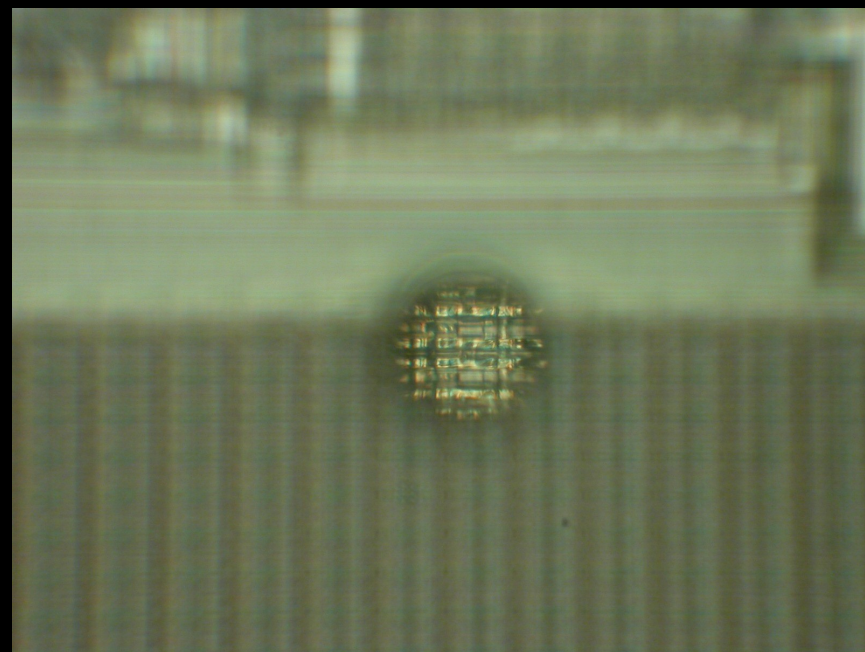
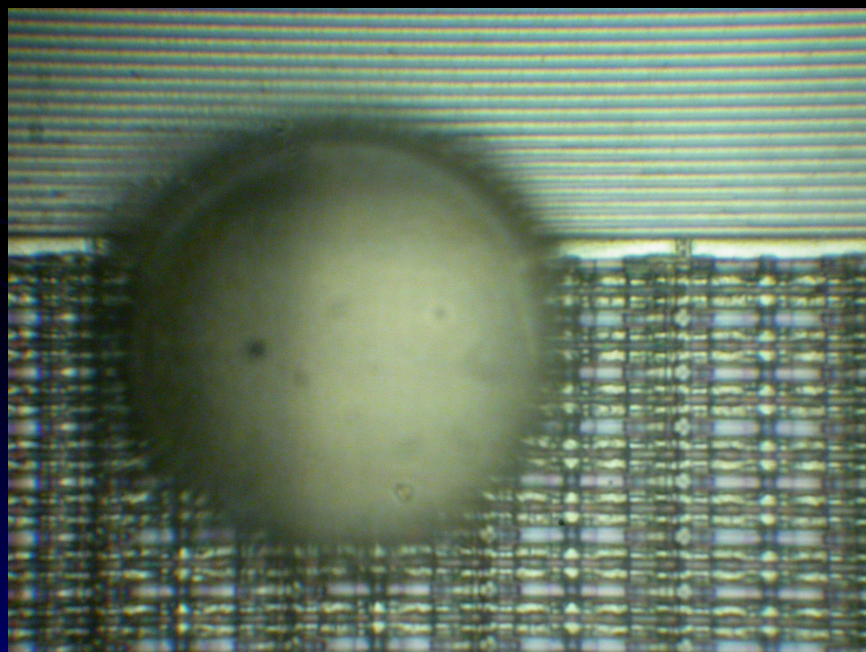


Motorola MC68HC705P6A microcontroller

# Semi-invasive attacks

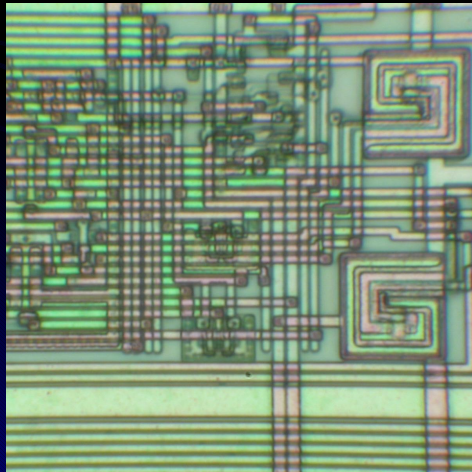
---

- Advanced imaging techniques
  - Using micro-lenses to increase NA of the optics
  - More effective for backside imaging increasing resolution to  $0.15\ \mu\text{m}$

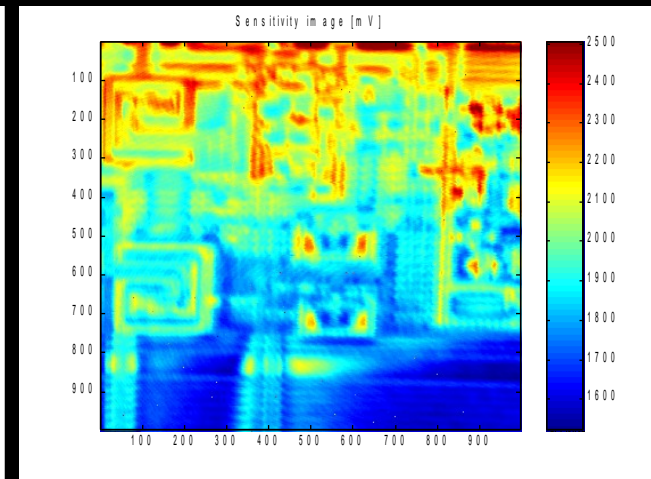
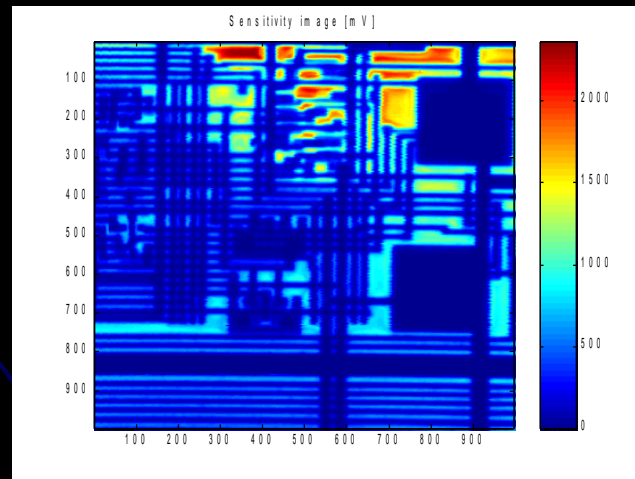


# Semi-invasive attacks

- 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)



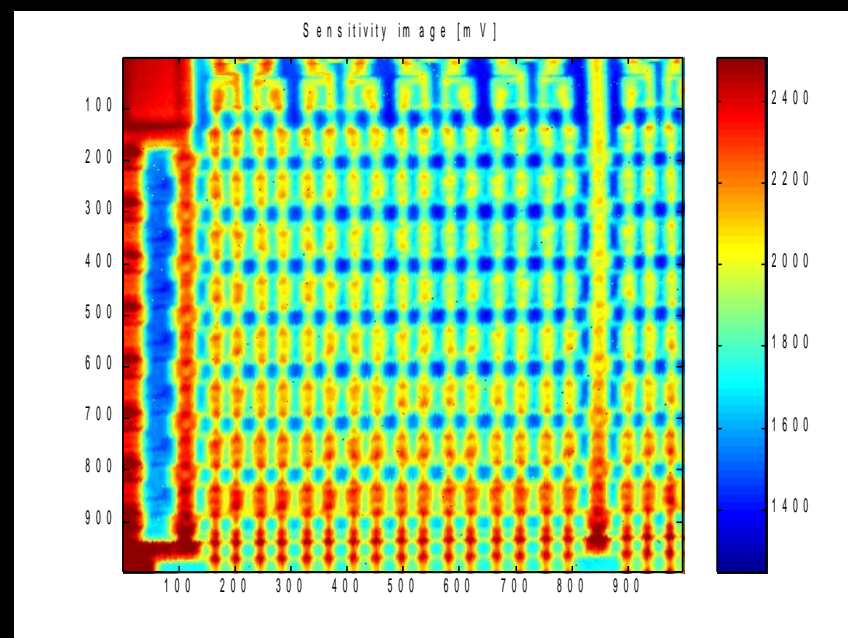
Microchip PIC16F84A microcontroller





# Semi-invasive attacks

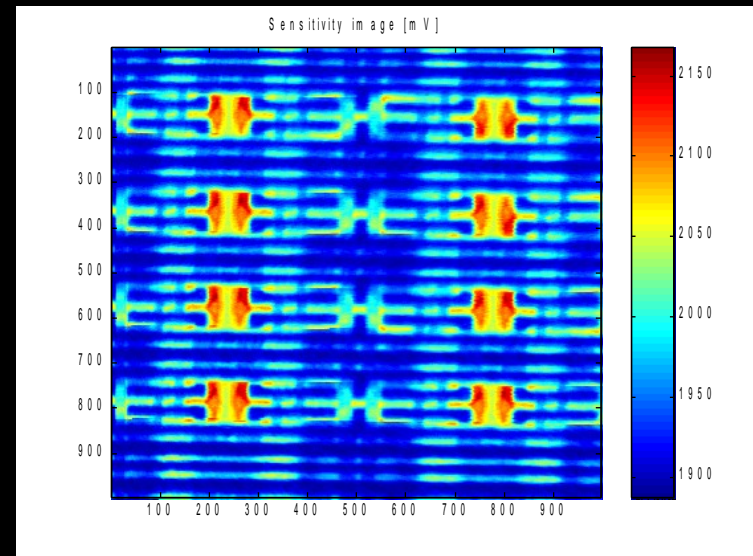
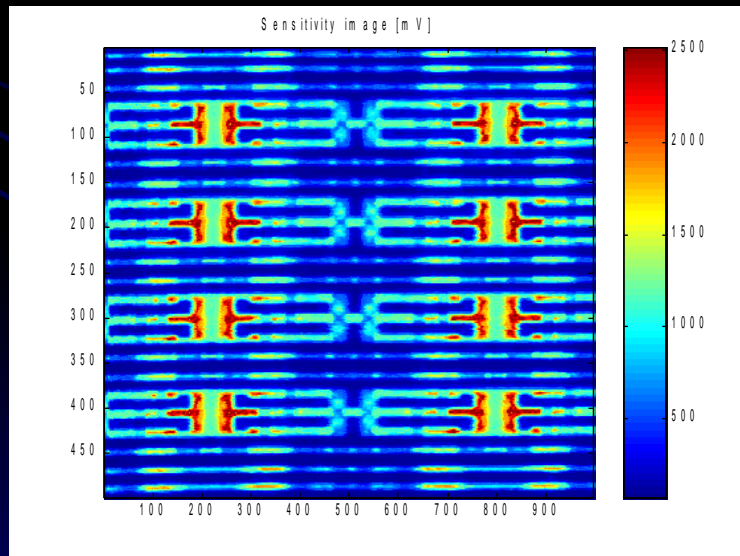
- Advanced imaging techniques – laser scanning
  - Mask ROM extraction without chemical etching
    - Also works from the rear side of a chip
    - Resolution is limited by wavelength of the infrared laser



Motorola MC68HC705P6A microcontroller

# Semi-invasive attacks

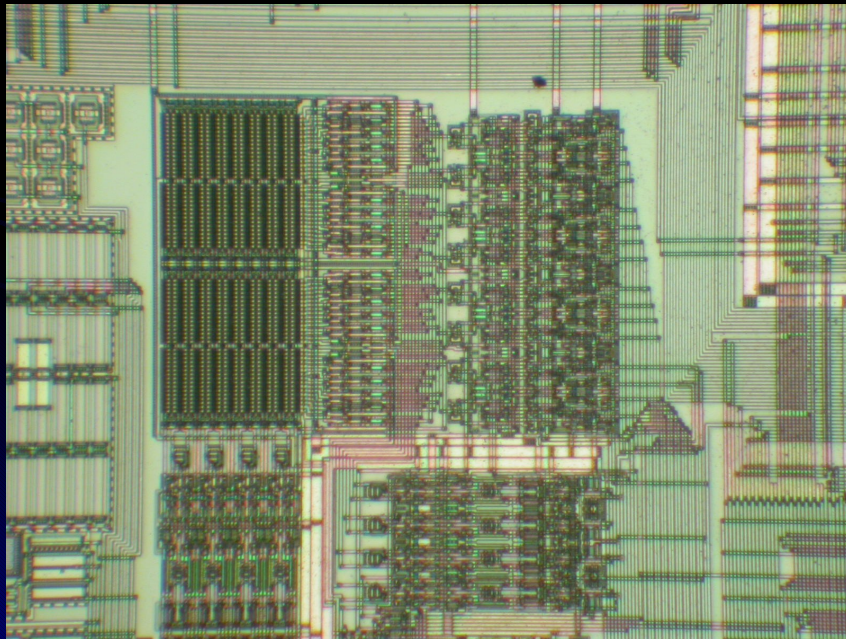
- Advanced imaging techniques – active photon probing
  - Light-induced current variation
    - Alternative to light-induced voltage alteration (LIVA) technique
    - Photon-induced photocurrent is dependable from the state of a transistor
    - Reading logic state of CMOS transistors inside a powered-up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



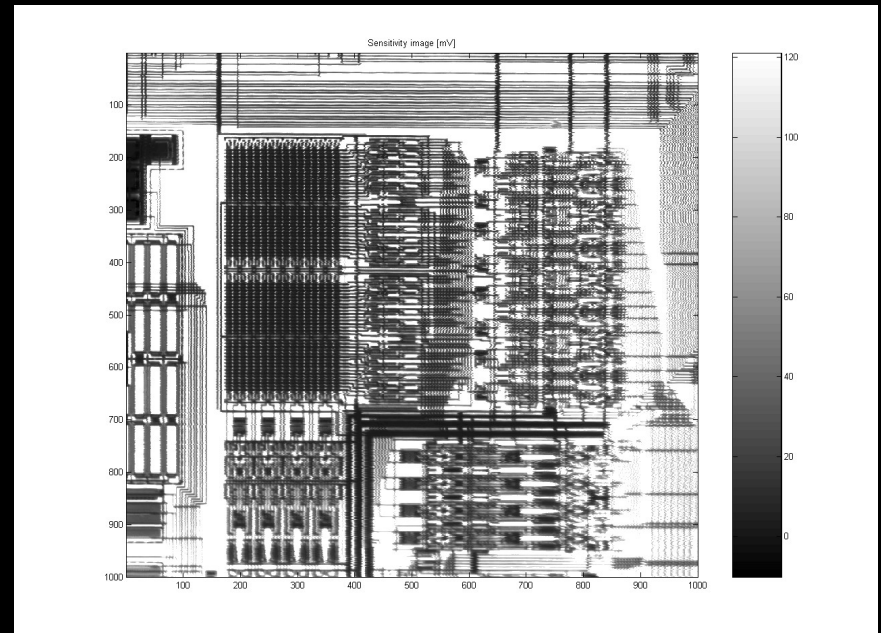
Microchip PIC16F84 microcontroller

# Semi-invasive attacks

- Data remanence in EEPROM and Flash memory devices
  - Using lasers to
    - monitor the state of memory transistors
    - influence cell characteristics ( $V_{TH}$ )
    - influence read-sense circuit ( $V_{ref}$ )

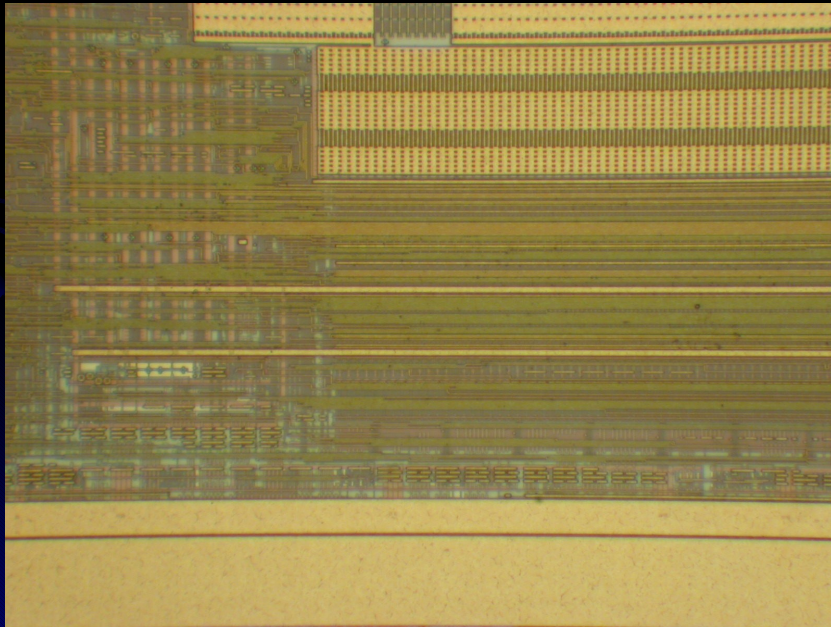


Microchip PIC16F84 microcontroller

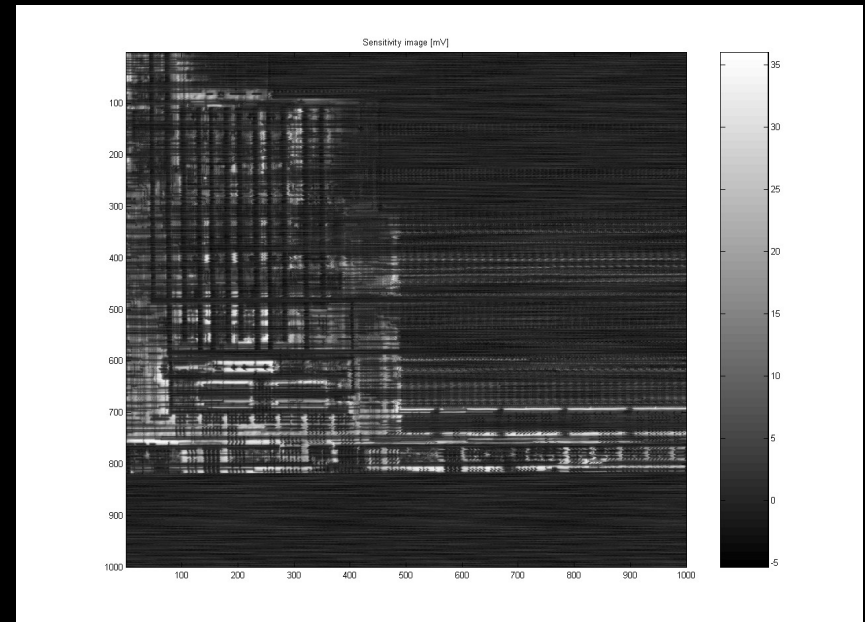


# Semi-invasive attacks

- Data remanence in EEPROM and Flash memory devices
  - Modern multilayer technologies (0.35  $\mu\text{m}$  or smaller process)
    - Three metal layers plus CMP makes it harder to attack the chip from its front side



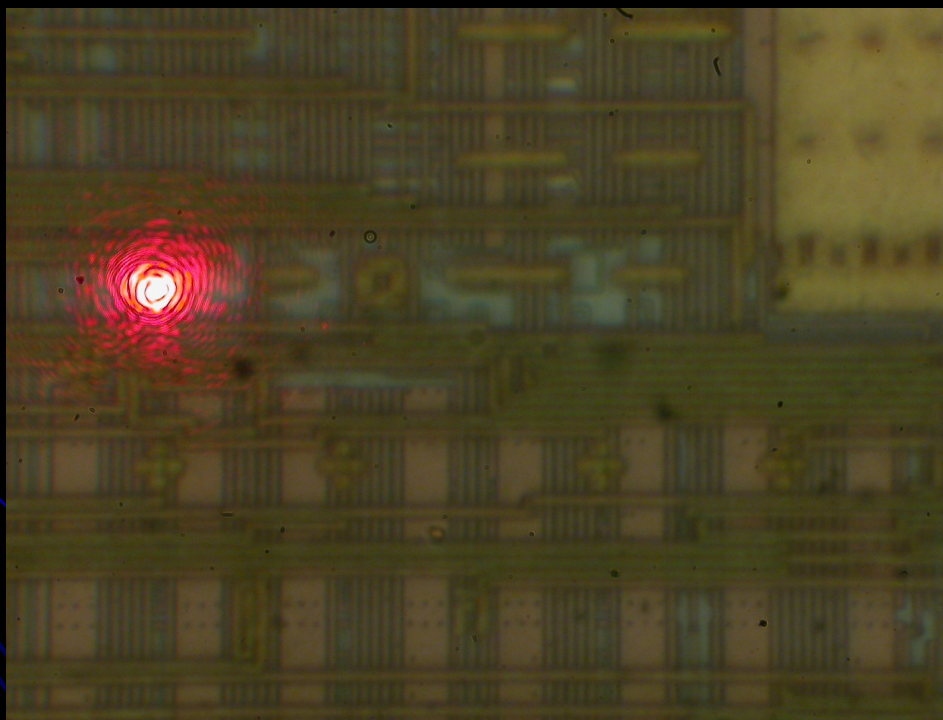
Atmel ATmega8 microcontroller



# Semi-invasive attacks

---

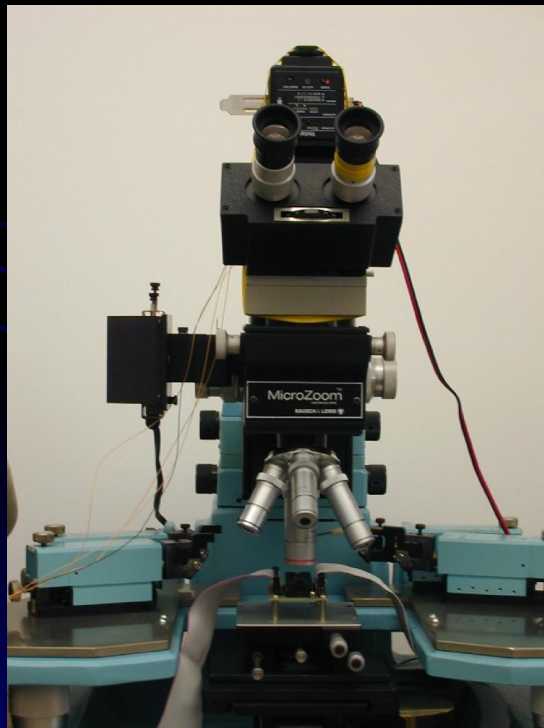
- Data remanence in Flash memory devices
  - Modern multilayer technologies (0.35  $\mu\text{m}$  or smaller process)
    - Rear side approach will be more effective



Atmel ATmega8 microcontroller

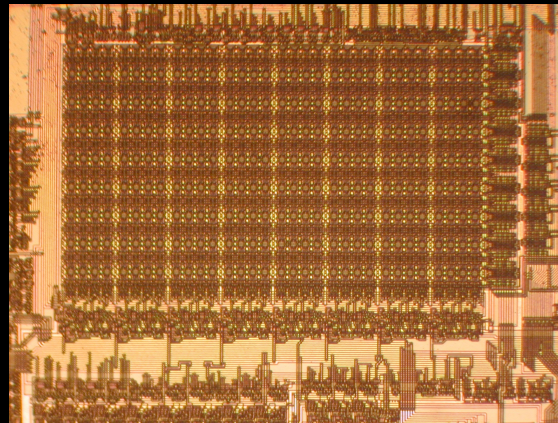
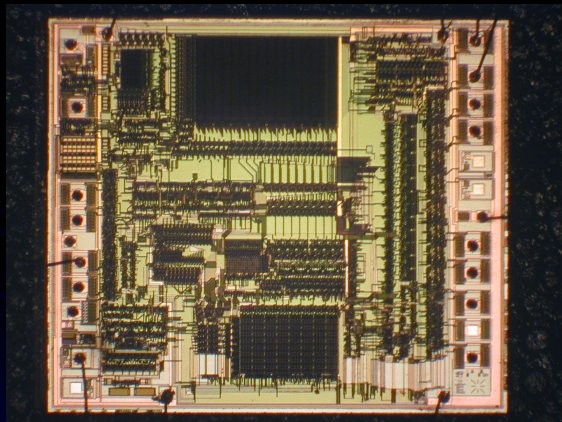
# Semi-invasive attacks

- Optical fault injection attacks
  - New class of attacks we introduced in 2002
  - Original setup involved optical microscope with a photoflash



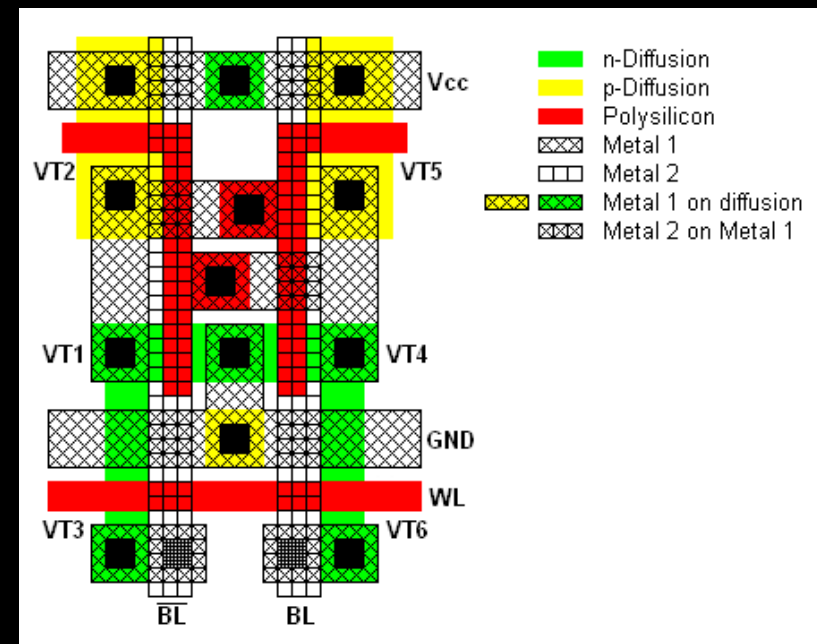
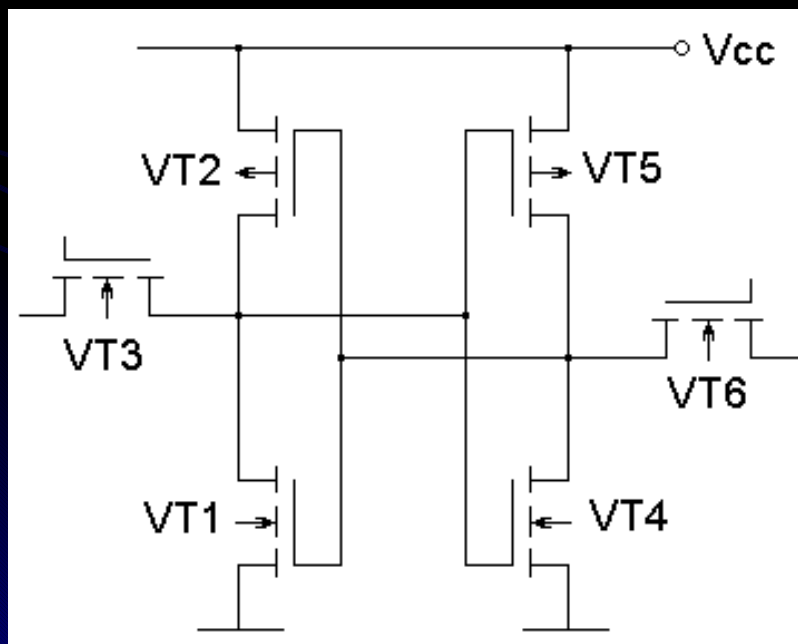
# Semi-invasive attacks

- Optical fault injection attack setup
  - The Microchip PIC16F84 microcontroller (1.2  $\mu\text{m}$  fabrication process) was programmed to monitor its internal SRAM
  - Magnification of the microscope was set to its maximum (1500 $\times$ )
  - Light from the photoflash was shielded with aluminium foil aperture



# Semi-invasive attacks

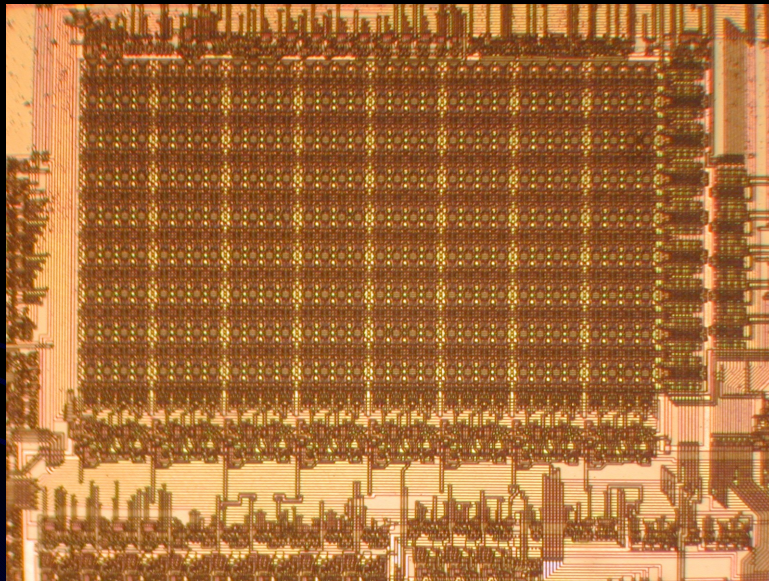
- Optical fault injection attacks
  - Intensive ionization opens closed transistor but does not influence opened transistor
  - The flip-flop can be switched by exposing closed n-channel transistor, causing the SRAM cell to change its state





# Semi-invasive attacks

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



B	B	B	B	B	B	B	B
I	I	I	I	I	I	I	I
T	T	T	T	T	T	T	T
7	6	5	4	3	2	1	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

---

- Improvements to the fault injection attack setup
  - Replacing the photoflash with a laser pointer
  - Using a motorised stage for easier control and analysis
  - Using the laser cutter system setup for fault injection
    - Laser pulses have fixed duration (5 – 8 ns)
    - The energy of pulses varies from pulse to pulse
  - Using specialised tools for optical fault evaluation (special laser microscopes designed specifically for optical fault probing)
    - Characterisation for the depth of focus
      - Chips with three and four metal layers very sensitive to the Z coordinate
    - Characterisation for different wavelengths and coordinates
      - Shorter wavelengths produce higher photocurrent
    - Characterisation for pulse duration
      - Long-distance effects for longer pulses (>100  $\mu$ s)

# Semi-invasive attacks

## ■ Comparing 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

## ■ Comparing with non-invasive attacks

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

# Conclusions

---

- There are many ways a given system can be attacked
  - Defender must protect against as many attacks as possible
- Technical progress helps both defenders and attackers
- Estimate attacker's experience and tools
- Security hardware engineers must be familiar with attack technologies to develop adequate protection
- Security protection of a system must be implemented at all levels, from hardware to software and human interface
- As attack technologies are constantly improving, secure hardware designs must be revised from time to time