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
- References
- Slides
  - http://www.cl.cam.ac.uk/~sps32/PartII_201109.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
  - electronic meters, phone cards, PayTV smartcards
  - crypto-processors and crypto-modules for encryption
  - many other devices and applications

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 for developers
  - design secure system (hardware security engineering task)
  - evaluate threats (how difficult is to break the protection?)
  - reduce the risk of being attacked and improve the security

Art of hardware security engineering

- What is the reason to attack your system?
  - attack scenarios and motivations
- Who is likely 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?
  - estimate the threat: understand motivation, cost and probability
  - develop adequate protection by locating weak points
  - perform security evaluation

Attack scenarios and motivations

- Cloning and overbuilding
  - copying for making profit without investment in development
  - low-cost mass production by subcontractors
- 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 a known weakness in the system
- Class II (knowledgeable insiders):
  - have substantial specialised technical education and experience
  - understand many parts of the system, have access to information
  - often have access to sophisticated tools 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

- Side-channel attacks
  - 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

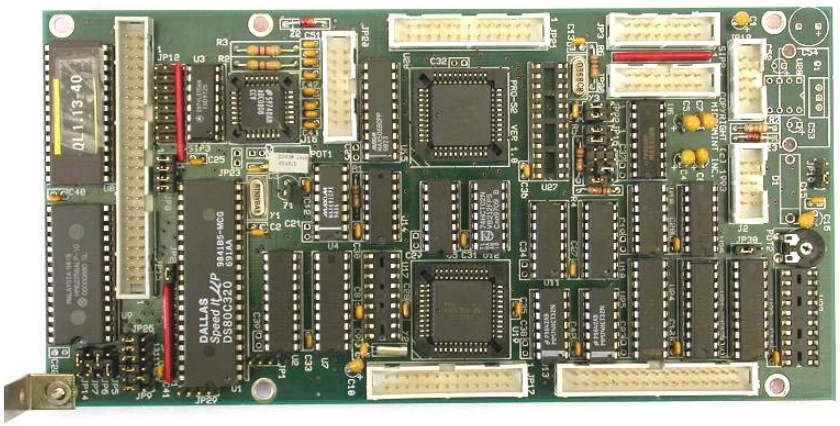
Attack methods

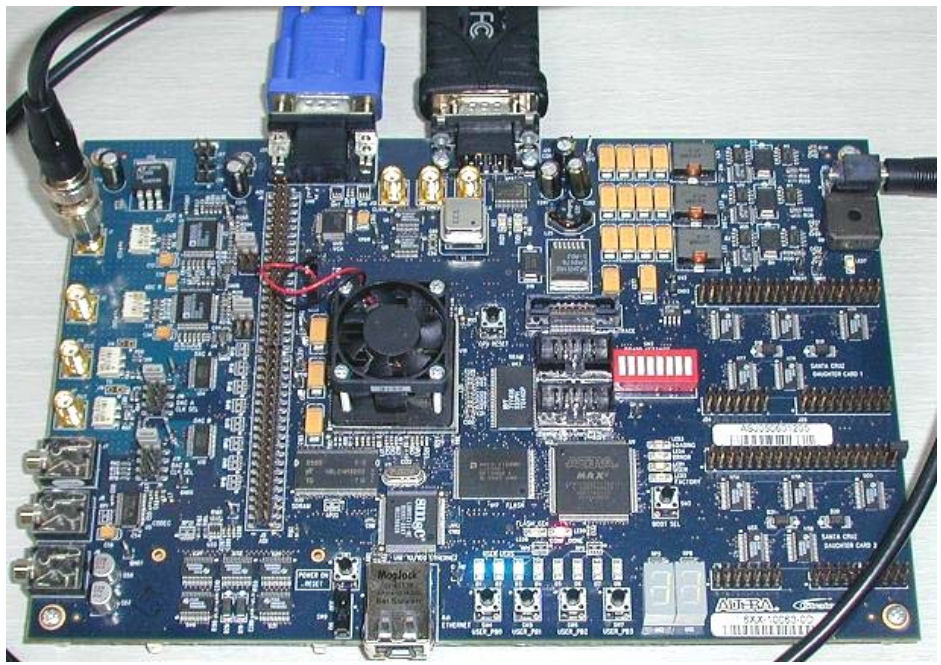
- Non-invasive attacks
  - observe or manipulate with the device without physical harm to it
  - require only moderately sophisticated equipment and knowledge to implement
- Invasive attacks
  - almost unlimited capabilities to extract information from chips and understand their functionality
  - normally 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

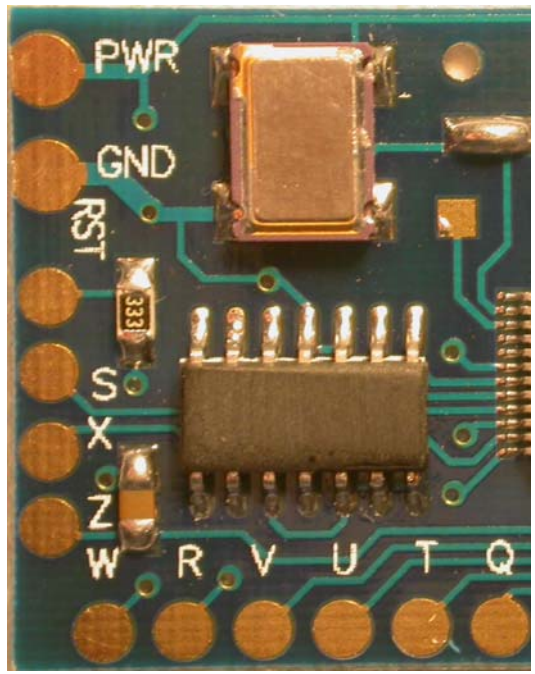
- Level ZERO (no special protection)
  - microcontroller or FPGA with external ROM
  - no special security features are used. All parts have free access and can be easily investigated
  - very low cost, attack time: minutes to hours





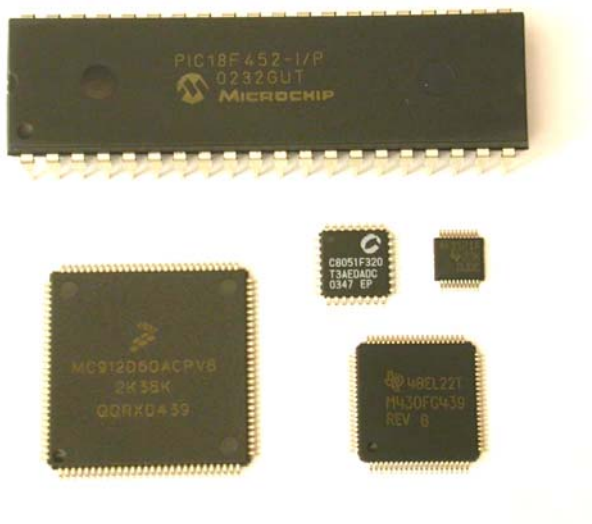
Tamper protection levels

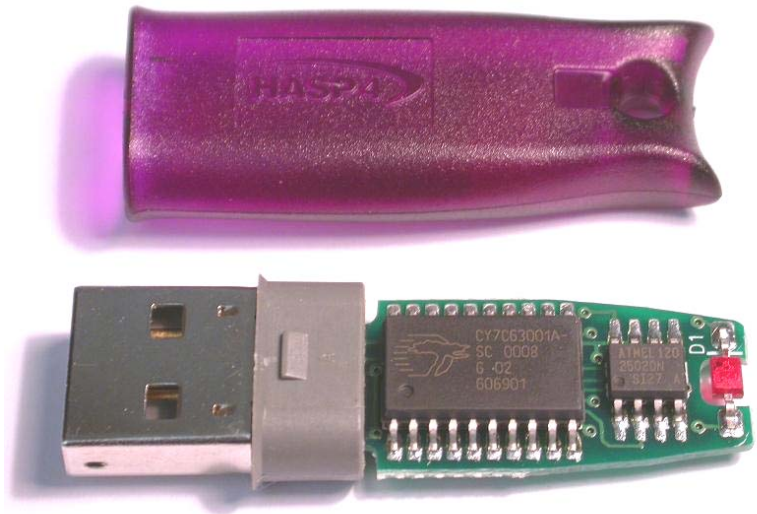
- Level LOW
  - microcontrollers with proprietary access algorithm, remarked ICs
  - some security features are used but they can be relatively easy defeated with minimum tools required
  - low cost, attack time: hours to days



Tamper protection levels

- Level MODL
  - microcontrollers with security protection, low-cost hardware dongles
  - protection against many low-cost attacks; relatively inexpensive tools are required for attack, but some knowledge is necessary
  - moderate cost, attack time: days to weeks



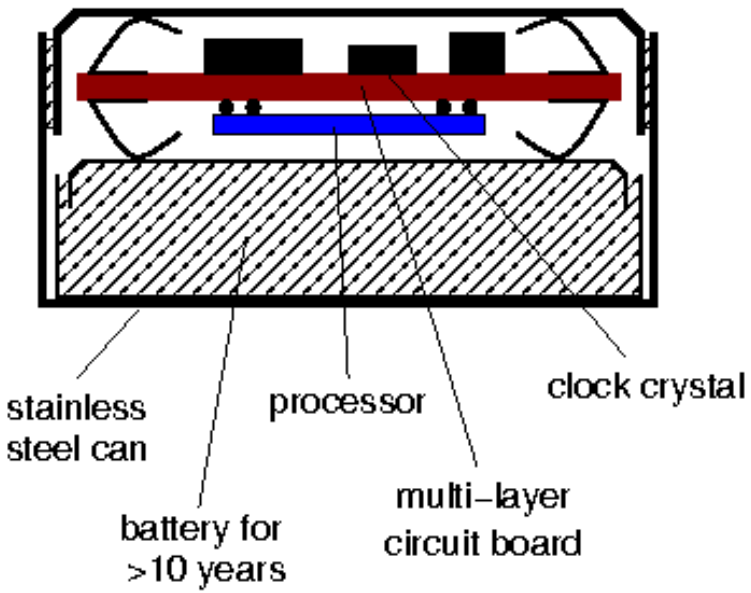


Tamper protection levels

- Level MOD
  - smartcards, high-security microcontrollers, ASICs, CPLDs, hardware dongles, i-Buttons, secure memory chips
  - special tools and equipment are required for successful attack as well as some special skills and knowledge
  - high cost, attack time: weeks to months

Tamper protection levels

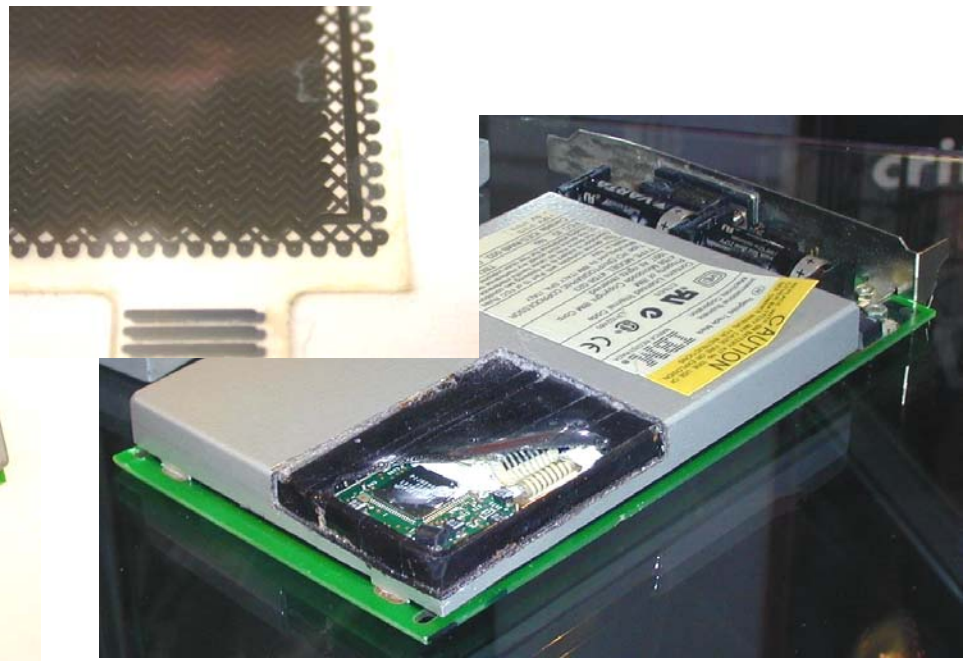
- Level MODH
  - secure i-Buttons, secure FPGAs, high-end smartcards, ASICs, custom secure ICs
  - special attention is paid to design of the security protection; equipment is available but is expensive to buy and operate
  - very high cost, attack time: months to years



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, attack time: years



Picture courtesy of Dr Markus Kuhn

Tamper protection levels

- Division into 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 products 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, FPGA board, prototyping boards
- Types of non-invasive attacks
  - timing, data remanence
  - side-channel attacks (power analysis, electro-magnetic analysis)
  - brute force, glitching

Non-invasive attacks

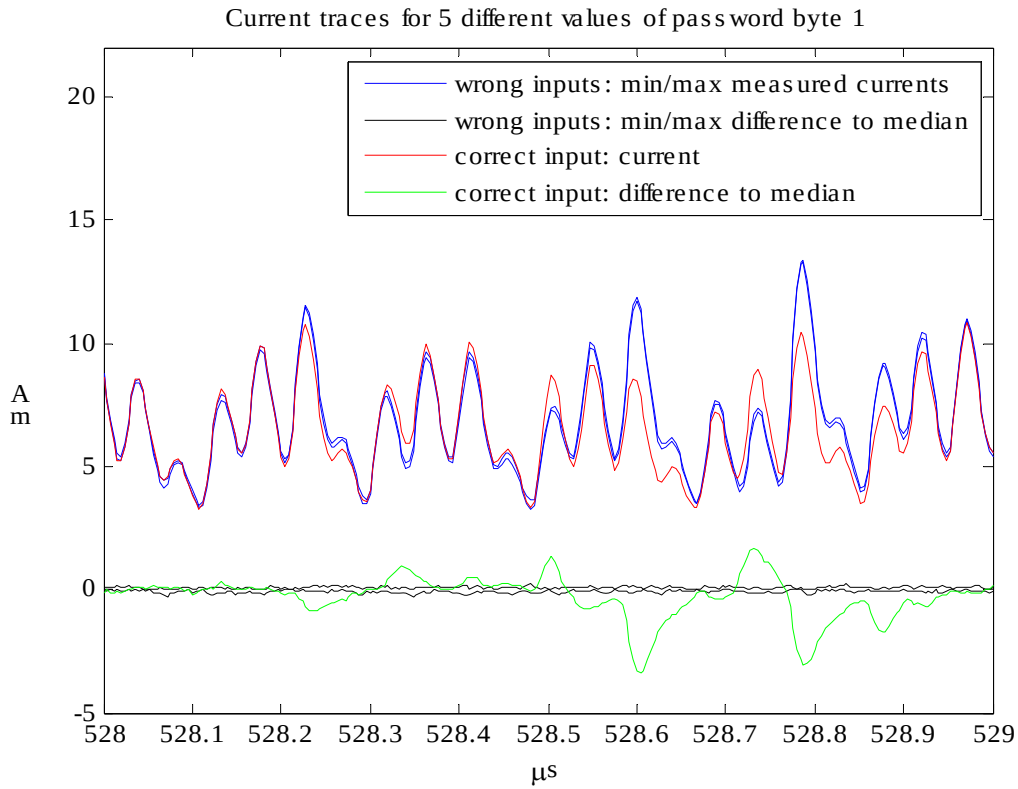
- Timing attacks aimed at different computation time
  - incorrect password verification
    - termination on incorrect byte
    - different computation length for incorrect bytes
  - incorrect implementation of encryption algorithms
    - performance optimisation (conditional branches)
    - cache memory usage
    - non-fixed time processor instructions (multiplication, division)
- Brute force attacks
  - searching for keys and passwords exploiting 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
  - very simple set of equipment – a PC with an oscilloscope and a small resistor in power supply line, 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
- Methods
  - simple power analysis (SPA): any differences in instruction flow
  - differential power analysis (DPA): any differences in data flow and correlation between data and secret

Non-invasive attacks

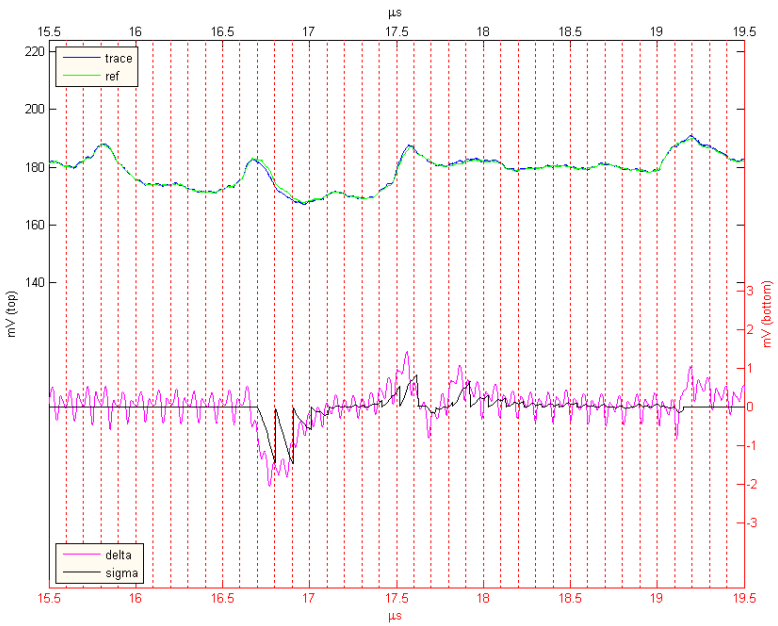
- Simple power analysis (SPA)
  - 8-byte password check in Freescale MC908AZ60A microcontroller
  - 1 byte at a time, 1 of 256 attempts leads to distinctive power trace
  - full password recovery in 2048 attempts (less than 10 minutes)

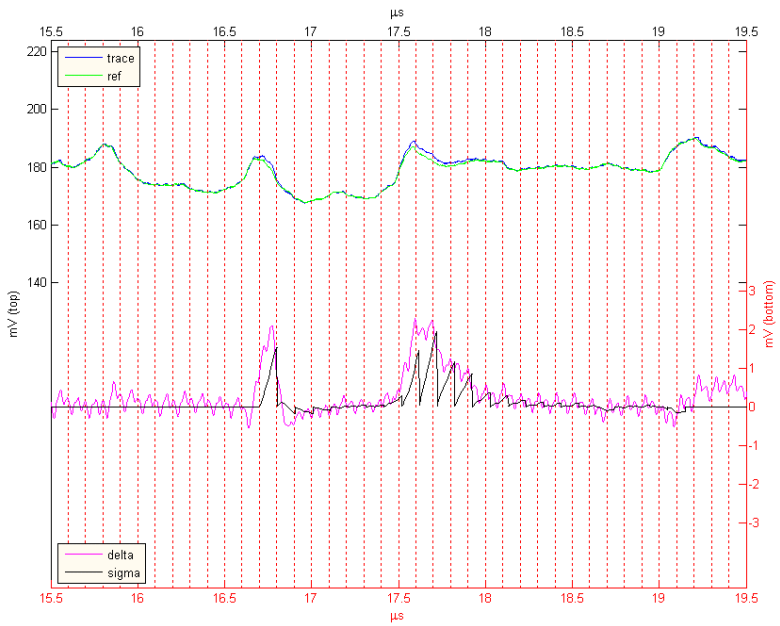



```
loop:   CBEQX #$FE, ptr3   ;check for end
        JSR sub_recv       ;receive byte
        CBEQ X+, ptr2      ;compare byte
        CLR adr_50         ;clear status
ptr1:   BRA loop           ;loop
ptr2:   BRA ptr1           ;time alignment
ptr3:   LDX #$FF           ;set address
        LDA adr_50         ;check status
        BEQ cont           ;skip flash enable
        STX , X            ;flash enable
cont:   … … …
```

Non-invasive attacks

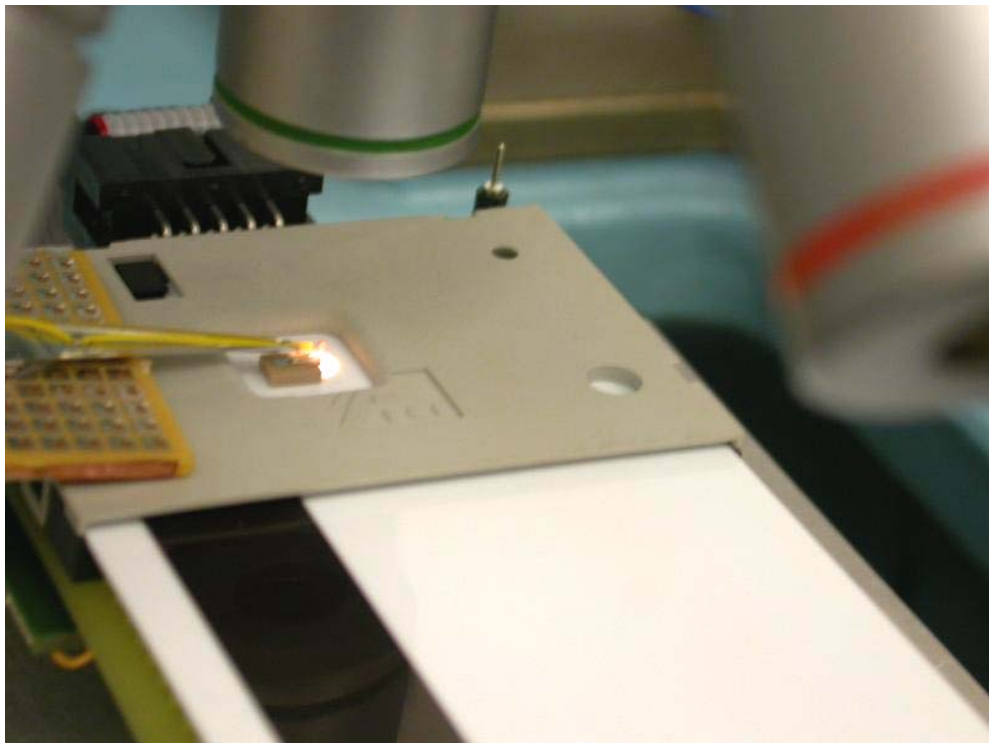
- Differential power analysis (DPA)
  - AES decryption in asynchronous ASIC (130 nm, 1.5V), 128-bit key
  - first round of decryption starts with XORing the input data with round key, the difference is only in the input data and the result
  - full key recovery in 256 attempts with each attempt requiring average of 4096 traces (~2 minutes per attempt, total 8 hours)





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



Non-invasive attacks

- Glitch attacks
  - clock glitches
  - power supply glitches
- Security fuse verification in the Mask ROM bootloader of the Motorola MC68HC05B6 microcontroller
  - double frequency clock glitch causes incorrect instruction fetch
  - low-voltage power glitch results in corrupted EEPROM data read

```
        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

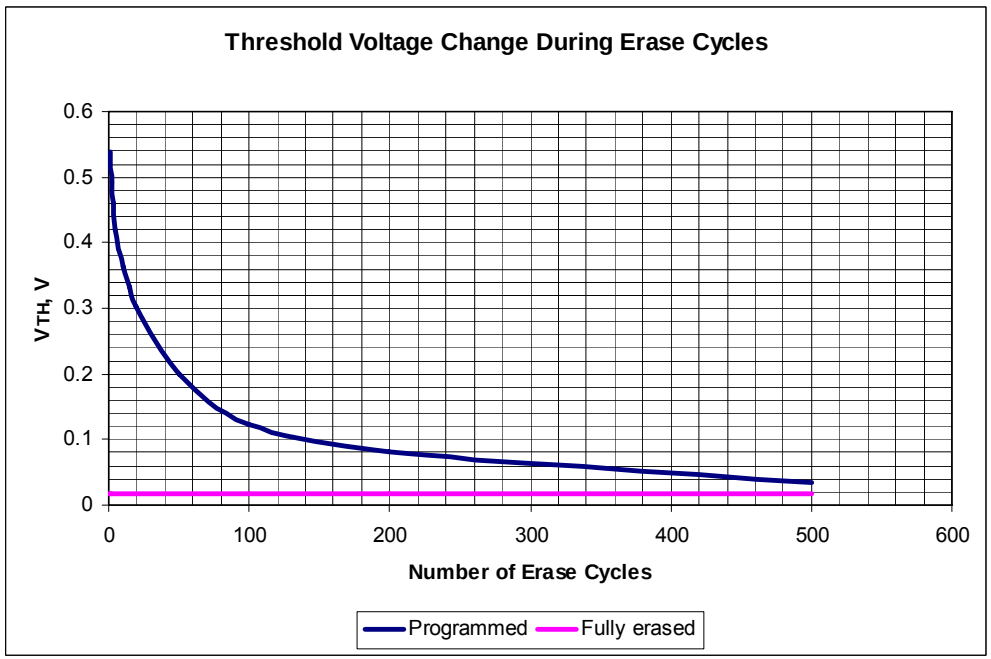
- Data remanence in SRAM
  - residual representation of data after erasure – first discovered in magnetic media then appeared to be the case for other memories
  - low temperature data remanence is dangerous to tamper resistant devices which store keys and secret data in a battery backed-up SRAM
  - long period of time data storage causes the data to be “burned-in” and likely to appear after power up; dangerous to secure devices which store keys at the same memory location for years
- Eight SRAM samples were tested at different conditions
  - at room temperature the retention time varies from 0.1 to 10 sec
  - cooling down to −20ºC increases the retention time to 1…1000 sec, while at −50ºC the data retention time is 10 sec to 10 hours
  - 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
    - use floating-gate transistors for storage, 10^3 – 10^5 e^-
  - Levels of remanence threat
    - file system (erasing a file → undelete)
    - file backup (software features)
    - smart memory (hardware buffers)
    - memory cell
  - Possible outcomes
    - circumvention of security in microcontrollers, FPGAs, smartcards
    - information leakage through shared EEPROM and Flash areas between different applications in secure chips

Non-invasive attacks

- Data remanence in EEPROM and Flash
  - threshold voltage of a memory cell (V_{TH}) is compared with reference voltage which is proportional to the power supply and can be influenced
  - memory bulk erase cycles
    - Flash memory, after 100 erase cycles: ΔV_{TH} = 100 mV
    - EEPROM memory, after 10 erase cycles: ΔV_{TH} = 1 mV
  - information successfully recovered from PIC16F84 after 10 erase cycles

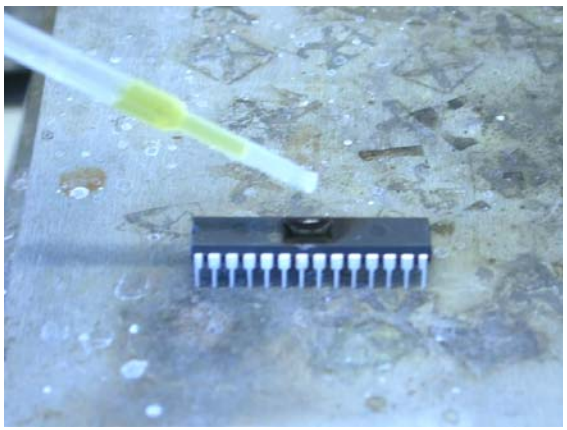


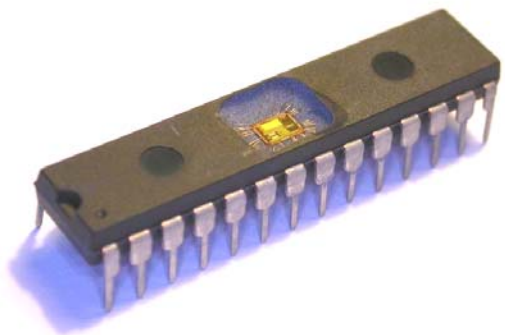
Invasive attacks

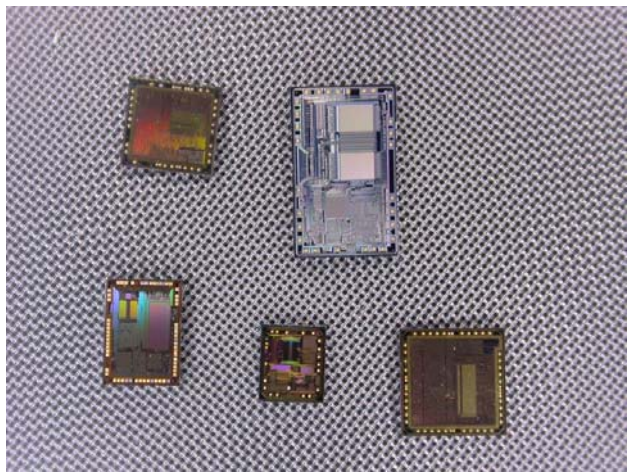
- Penetrative attacks
  - leave tamper evidence of the attack or even destroy the device
- Tools
  - IC soldering/desoldering station
  - simple chemical lab
  - high-resolution optical microscope
  - wire bonding machine, laser cutting system, microprobing station
  - oscilloscope, logic analyser, signal generator
  - PC with data acquisition board, FPGA board, prototyping boards
  - scanning electron microscope (SEM)
  - focused ion beam (FIB) workstation
- Types of invasive attacks
  - decapsulation, optical imaging, reverse engineering
  - microprobing, deprocessing, modification

Invasive attacks

- Sample preparation: decapsulation
  - manual with fuming nitric acid (HNO_3) and acetone at 60ºC
  - automatic using mixture of HNO_3 and H_2SO_4
  - full or partial from front side and rear side

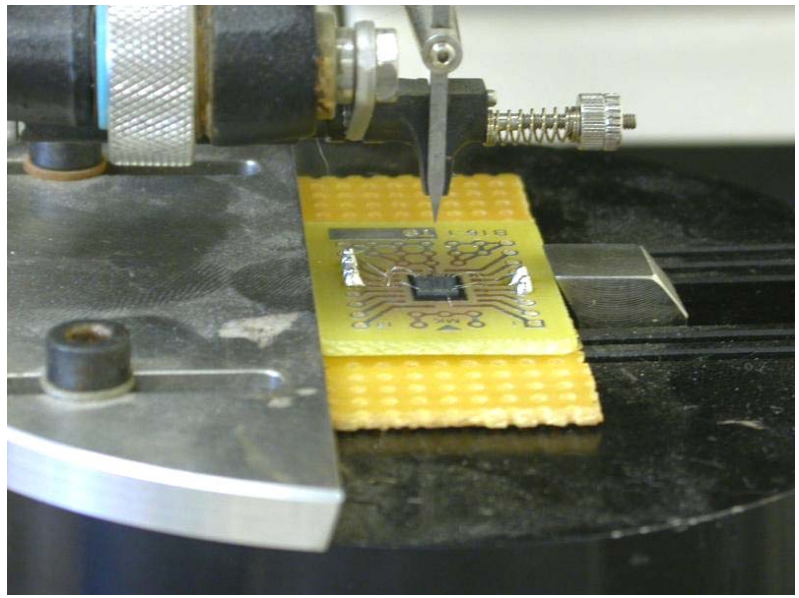






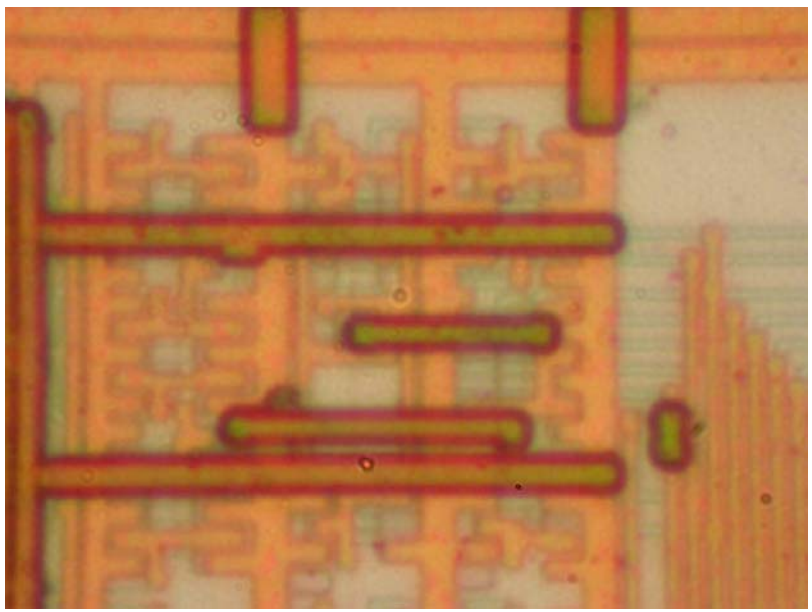
Invasive attacks

- Sample preparation: bonding
  - wedge wire bonder
  - gold ball bonder

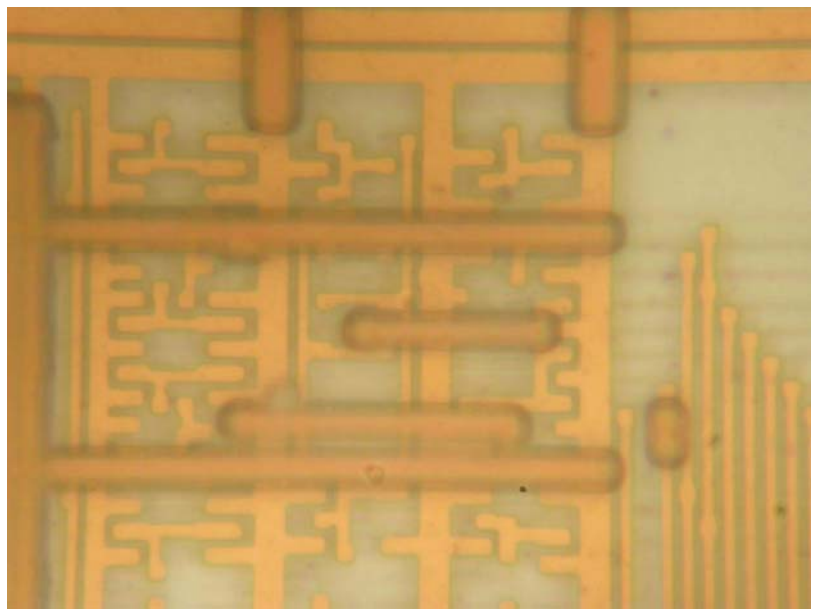


Invasive attacks

- Optical imaging
  - resolution is limited by optics and wavelength of a light:
    $R = 0.61\,\lambda / NA = 0.61\,\lambda / n \sin(\mu)$
    - reduce wavelength of the light using UV sources
    - increasing the angular aperture, e.g. dry objectives have $NA = 0.95$
    - increase refraction index of the media using immersion oil ($n = 1.5$)



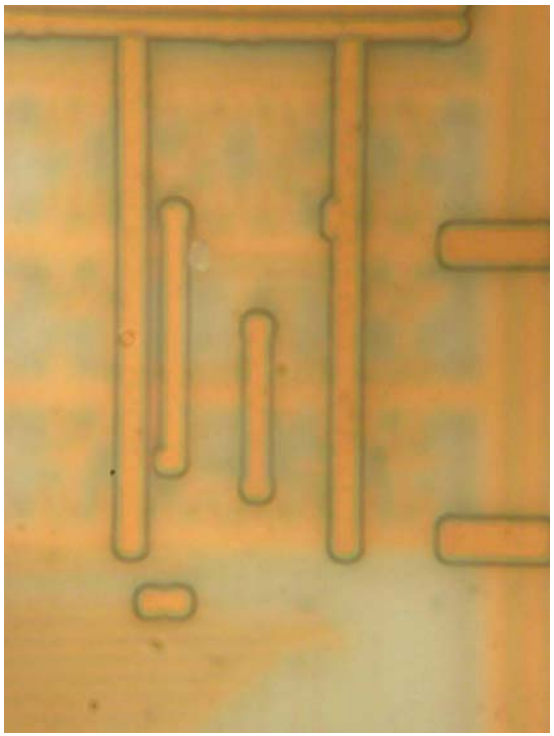
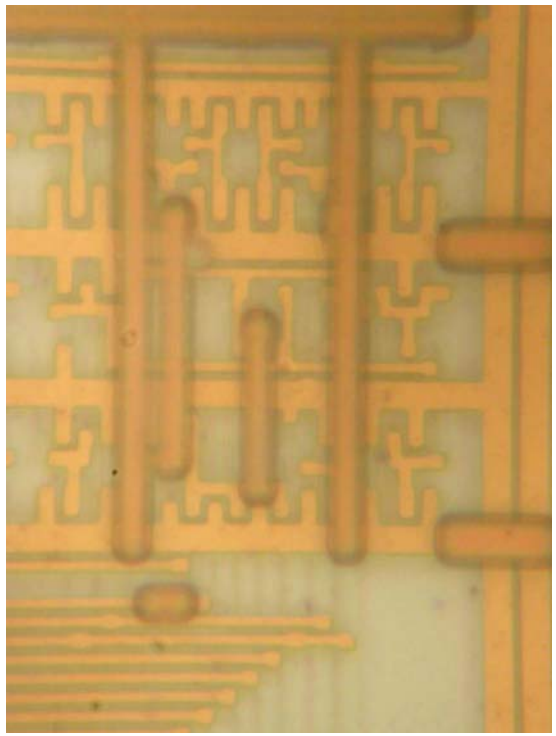
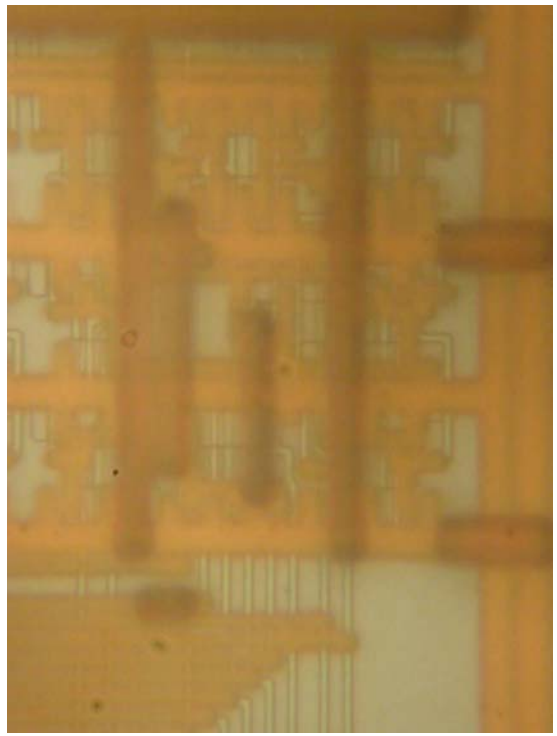
Bausch&Lomb MicroZoom, 50×2×, NA = 0.45



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 post-processing

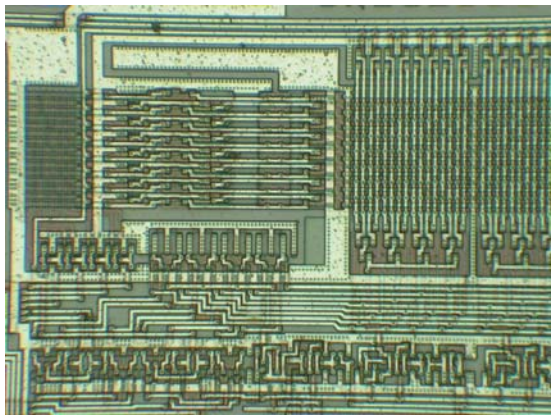




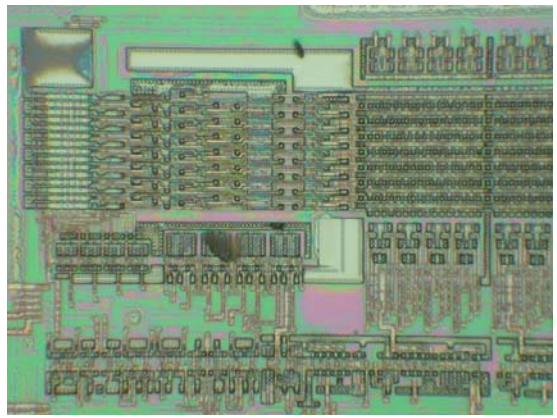
Invasive attacks

- Deprocessing
  - removing passivation layer to expose 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

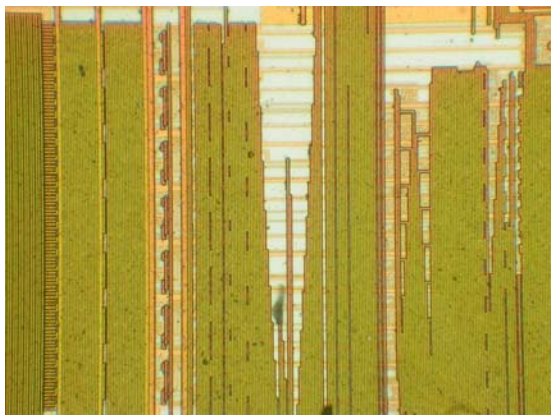
- Removing top metal layer using wet chemical etching
  - good uniformity over the surface, but works reliably only for chips fabricated with 0.8 µm or larger process (without polished layers)

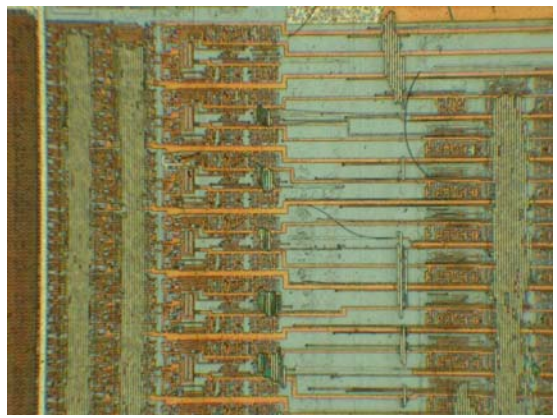




Motorola MC68HC705C9A microcontroller

1.0 µm



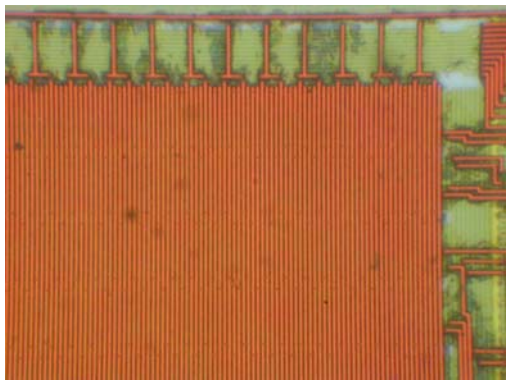


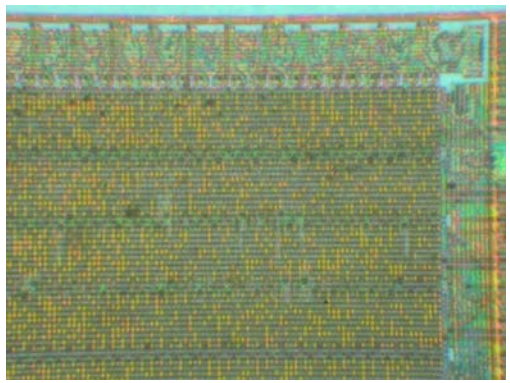
Microchip PIC16F76 microcontroller

0.5 µm

Invasive attacks

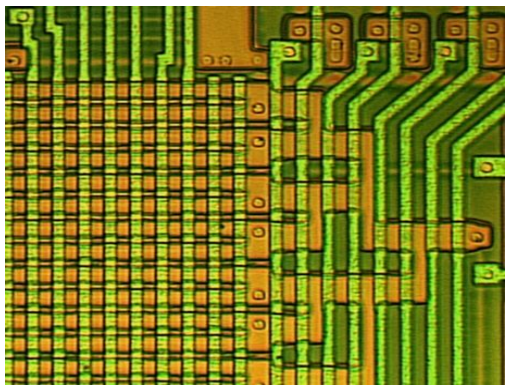
- Memory extraction from Mask ROMs
  - removing top metal layers for direct optical observation of data in NOR ROMs (bits programmed by presence of transistors)
  - not suitable for VTROM (ion implanted) used in smartcards – selective (dash) etchants are required to expose the ROM bits

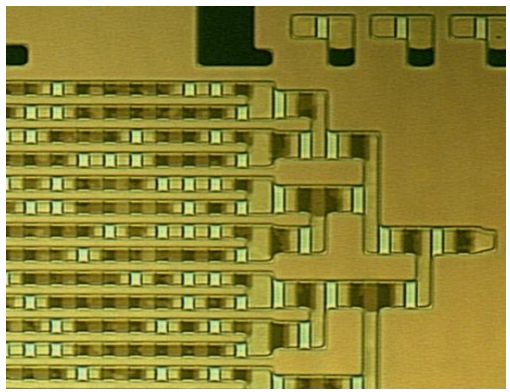




NEC μPD78F9116 microcontroller

0.35 μm





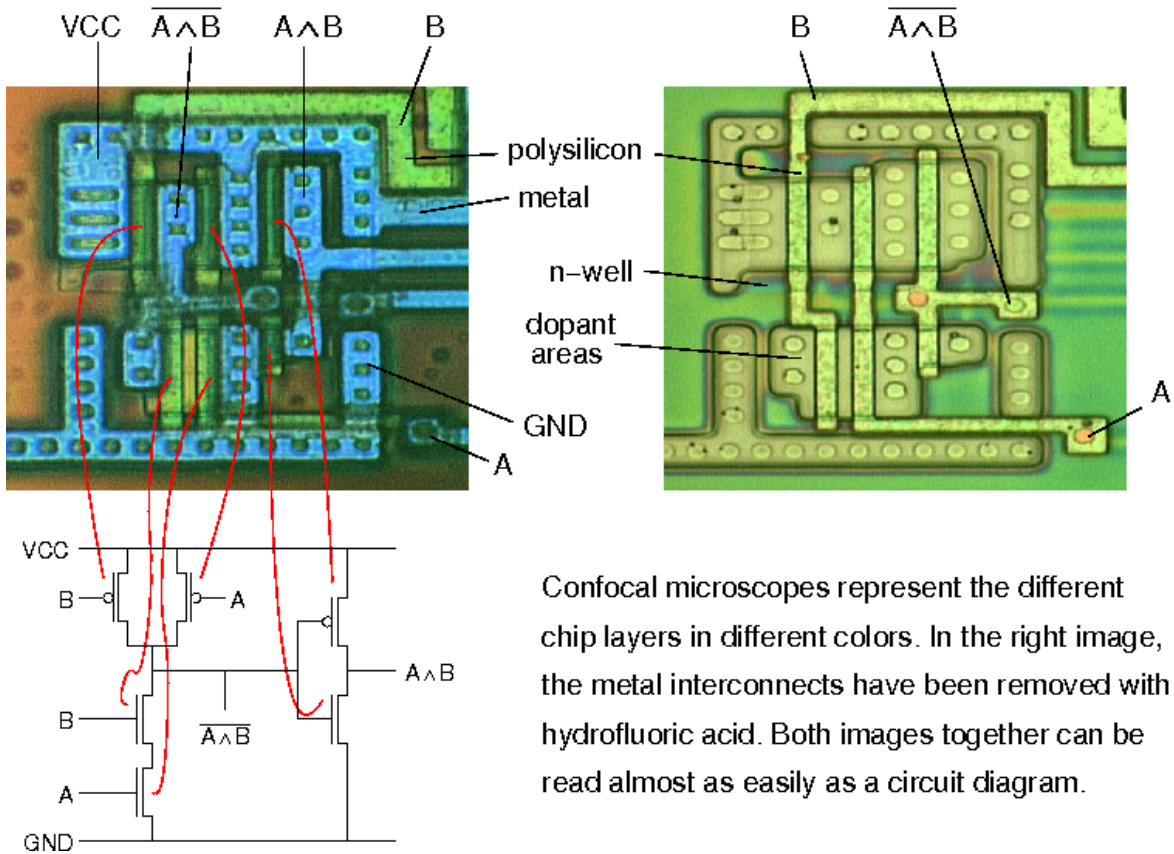
Motorola MC68HC05SC27 smartcard

1.0 μm

Picture courtesy of Dr Markus Kuhn

Invasive attacks

- Reverse engineering – understanding the structure of a semiconductor device and its functions
  - optical, using a confocal microscope (for > 0.5 µm chips)
  - deprocessing is necessary for chips with smaller technology

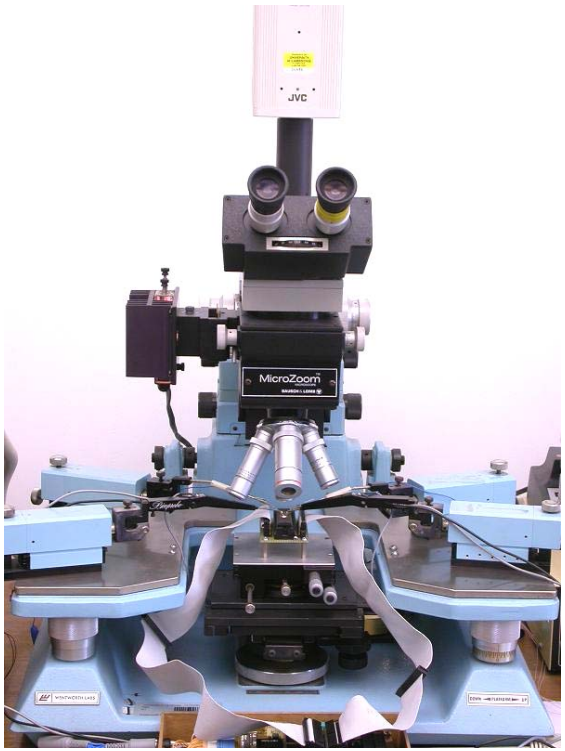


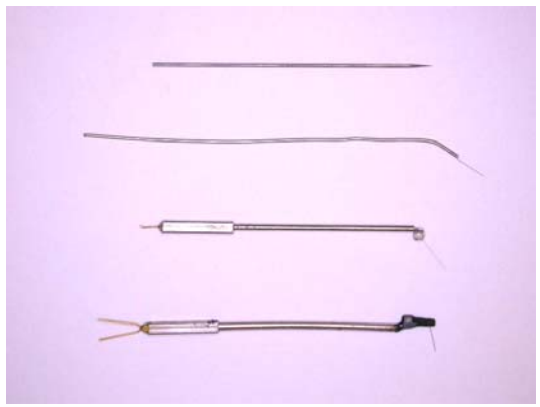
Confocal microscopes represent the different chip layers in different colors. In the right image, the metal interconnects have been removed with hydrofluoric acid. Both images together can be read almost as easily as a circuit diagram.

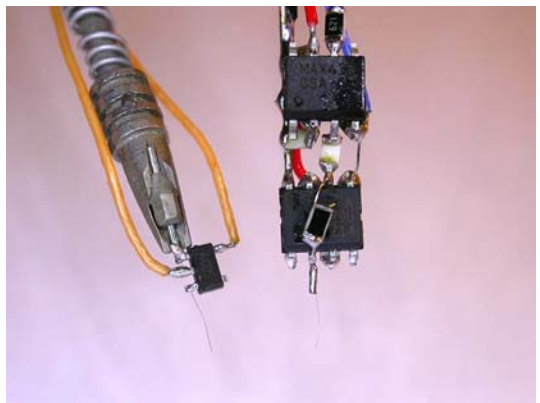
Picture courtesy of Dr Markus Kuhn

Invasive attacks

- Microprobing with fine electrodes
  - eavesdropping on signals inside a chip
  - injection of test signals and observing the reaction
  - can be used for extraction of secret keys and memory contents

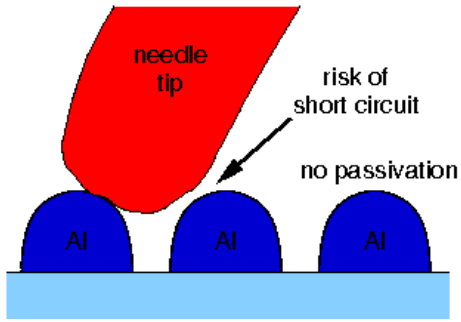


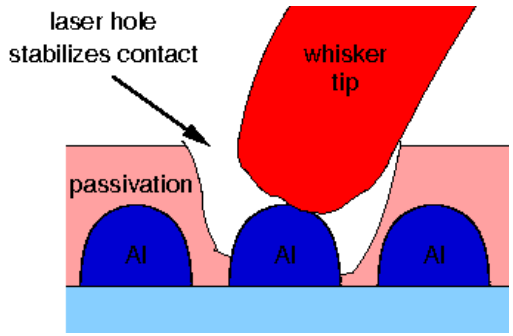




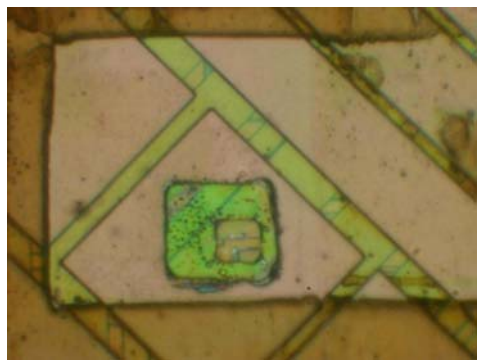
Invasive attacks

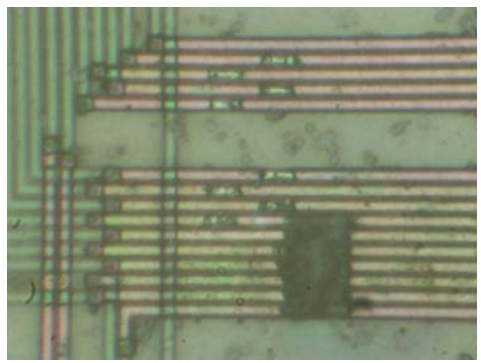
- Laser cutting systems
  - removing polymer layer from a chip surface
  - local removing of a passivation layer for microprobing attacks
  - cutting metal wires inside a chip





Picture courtesy of Dr Markus Kuhn

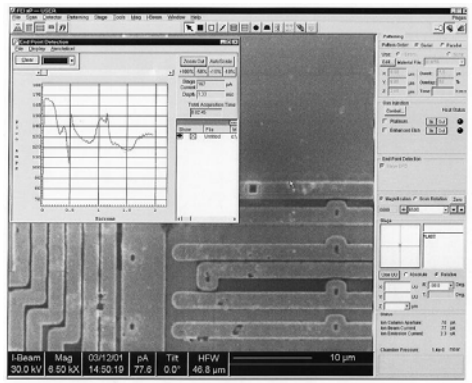


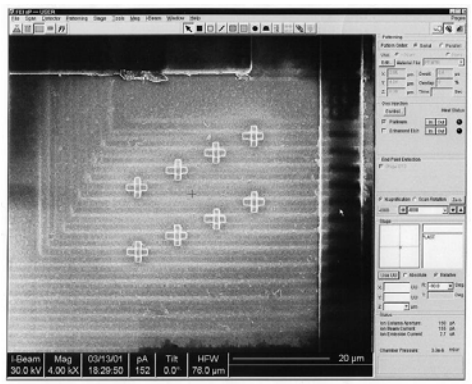


Invasive attacks

- Focused Ion Beam (FIB) workstation
  - chip-level surgery with 10 nm precision
  - etching with high aspect ratio
  - platinum and SiO_2 deposition

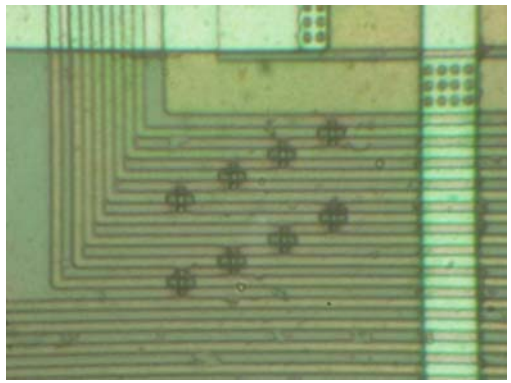
Picture courtesy of Semiresearch Ltd

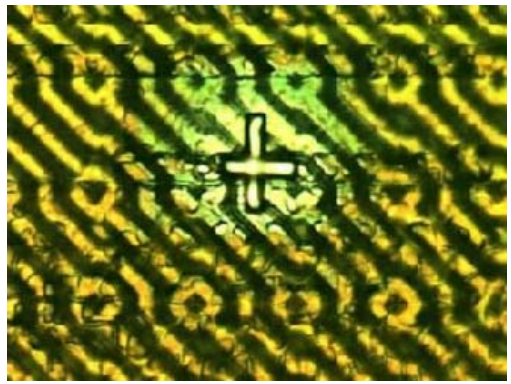




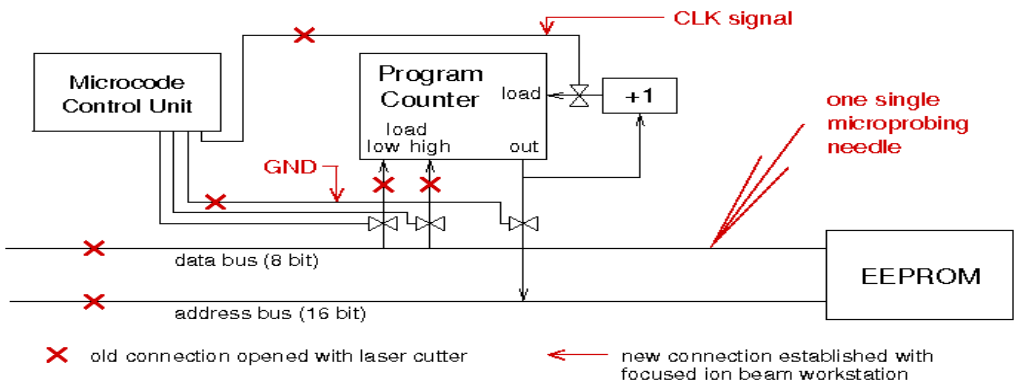
Invasive attacks

- Focused Ion Beam workstation
  - creating probing points inside smartcard chips, read the memory
  - modern FIBs allow backside access, but requires special chip preparation techniques to reduce the thickness of silicon





Picture: Oliver Kömmerling



Picture courtesy of Dr Markus Kuhn

Semi-invasive attacks

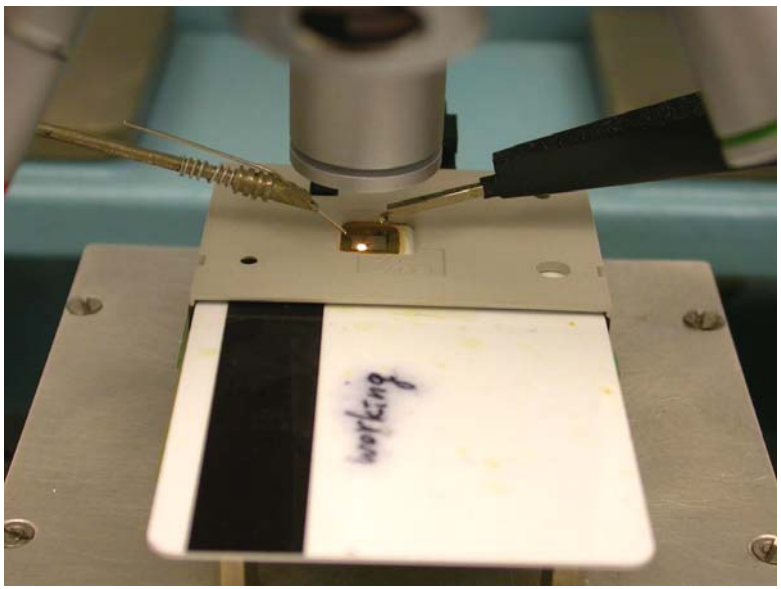
- Filling the gap between non-invasive and invasive attacks
  - less damaging to target device (decapsulation without penetration)
  - less expensive and easier to setup and repeat than invasive attacks
- Tools
  - IC soldering/desoldering station
  - simple chemical lab
  - high-resolution optical microscope
  - UV light sources, lasers
  - oscilloscope, logic analyser, signal generator
  - PC with data acquisition board, FPGA board, prototyping boards
  - special microscopes (laser scanning, infrared etc.)
- Types of semi-invasive attacks
  - UV attack, imaging, fault injection

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-ray attacks (without even opening the chip package)
  - interference with strong and localised electromagnetic fields

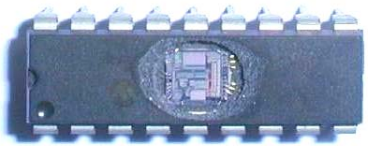
Semi-invasive attacks

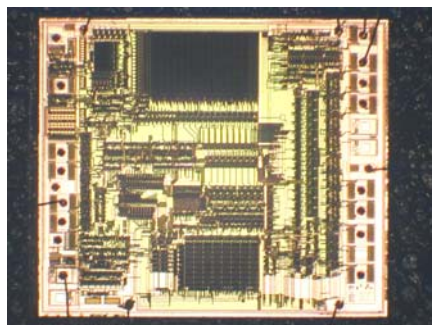
- Optical fault injection attacks
  - optical fault injection was observed in my experiments with microprobing attacks in early 2001, introduced as a new method in 2002
  - lead to new powerful attack techniques and forced chip manufacturers to rethink their design and bring better protection
  - original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

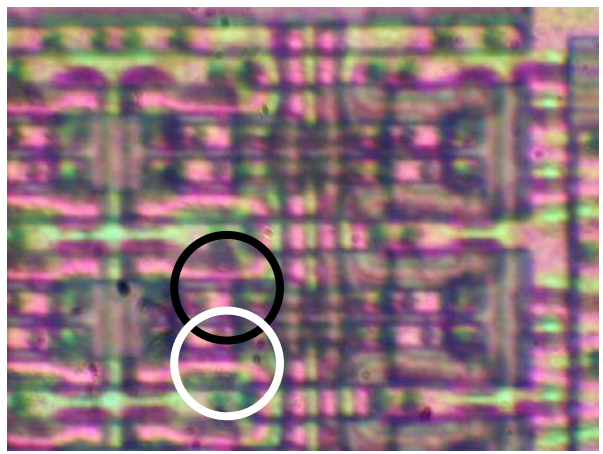


Semi-invasive attacks

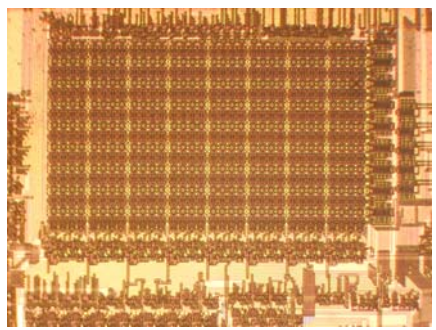
- Optical fault injection attack setup
  - Microchip PIC16F84 microcontroller (1.2 μm fabrication process) was programmed to monitor its internal SRAM
  - the chip was decapsulated and placed under a microscope
  - light from the photoflash was shaped with aluminium foil aperture
  - physical location of each memory address by modifying memory contents





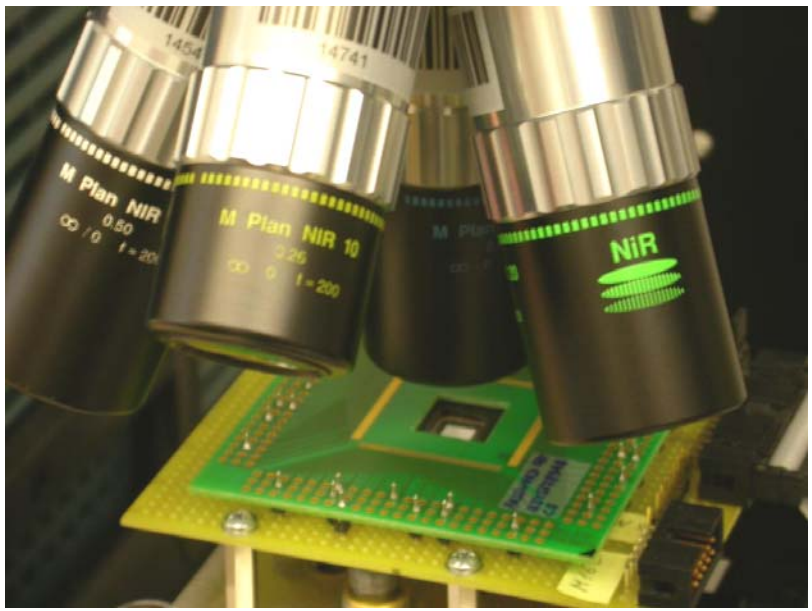


BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0



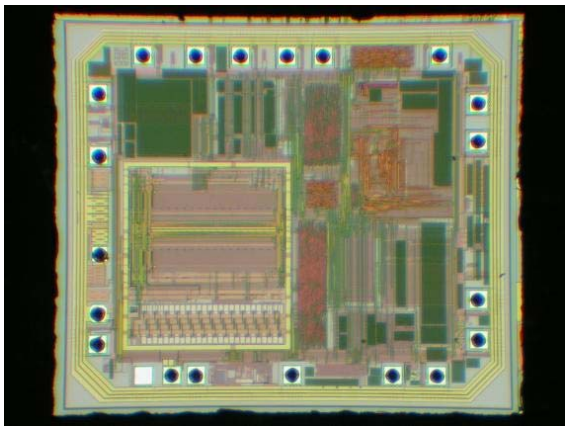
Semi-invasive attacks

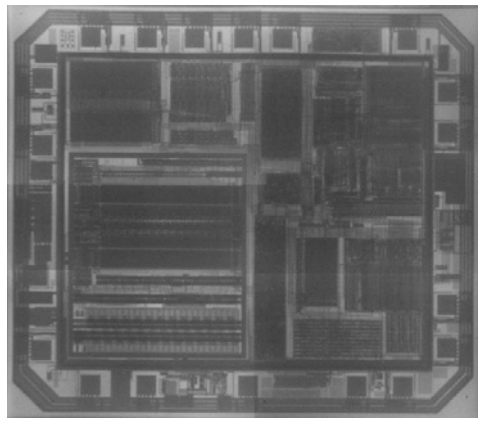
- Backside infrared imaging
  - microscopes with IR optics give better quality of image
  - IR-enhanced CCD cameras or special cameras must be used
  - resolution is limited to ~0.6 μm by the wavelength of used light



Semi-invasive attacks

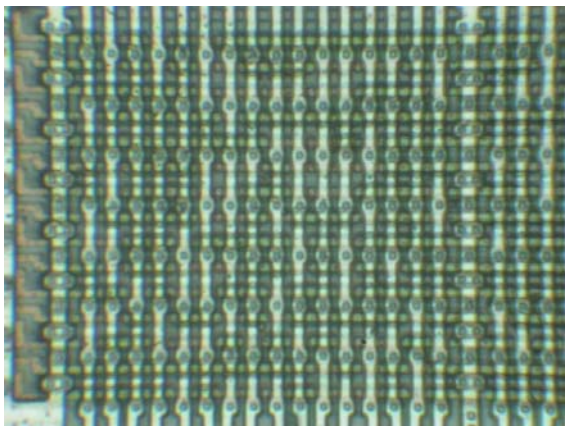
- Backside infrared imaging
  - view is not obstructed by multiple metal layers
  - reflected and transmitted light illumination can be used
  - Mask ROM extraction without chemical etching

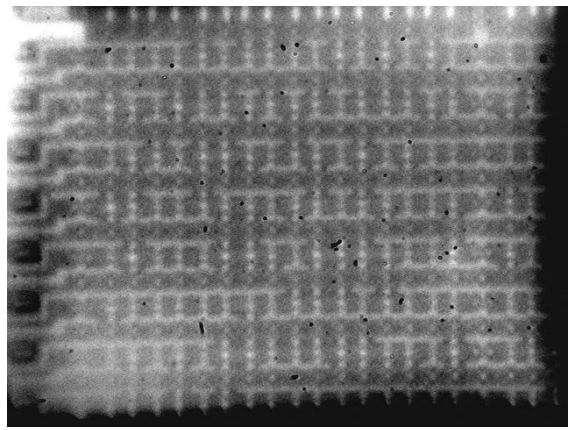




Texas Instruments MSP430F112 microcontroller

0.35 µm



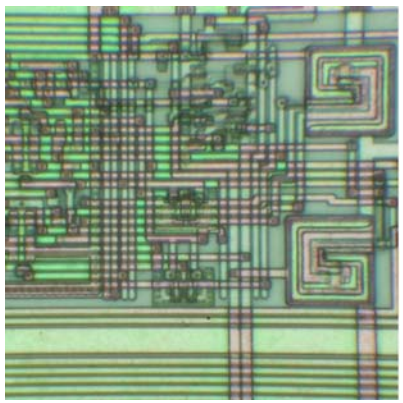


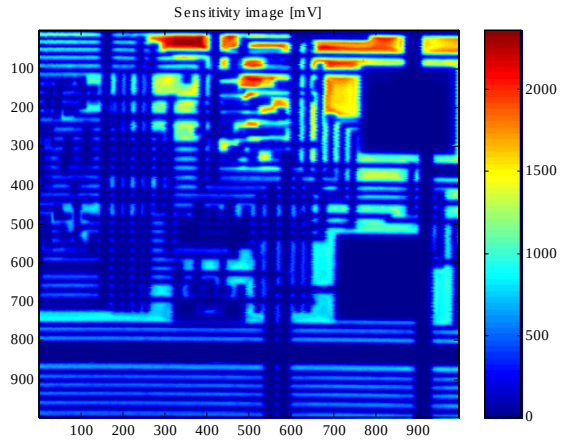
Motorola MC68HC705P6A microcontroller

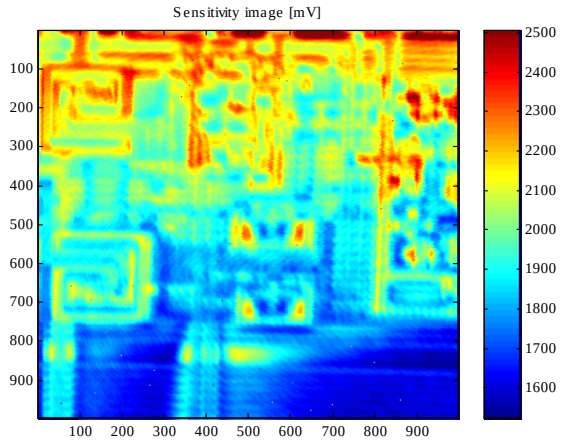
1.2 µm

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)



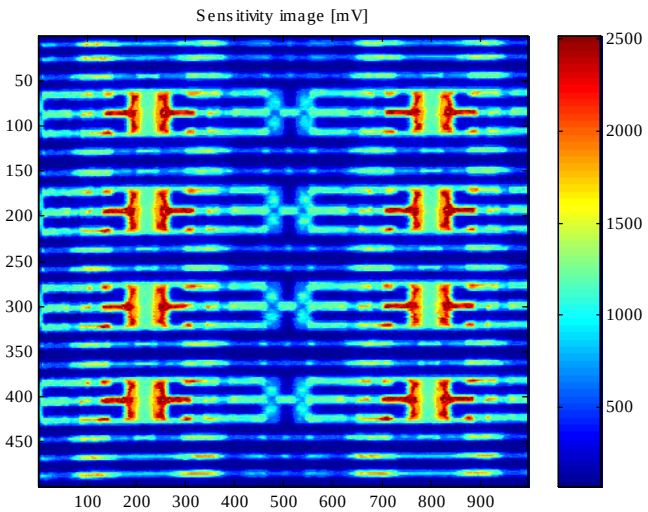


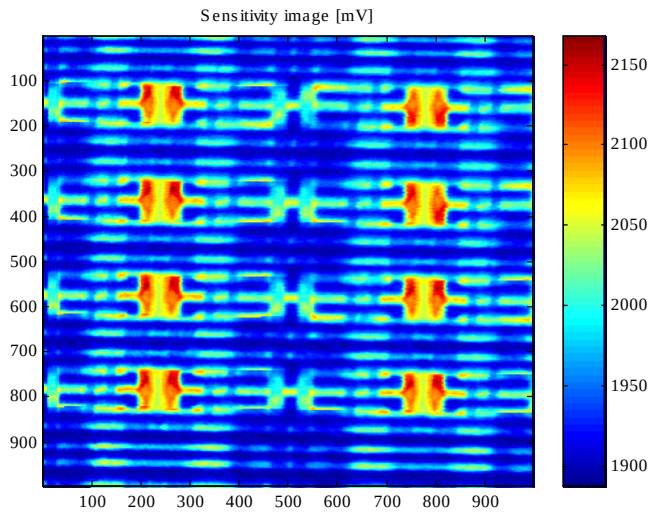


Microchip PIC16F84A microcontroller

Semi-invasive attacks

- Advanced imaging techniques – 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)

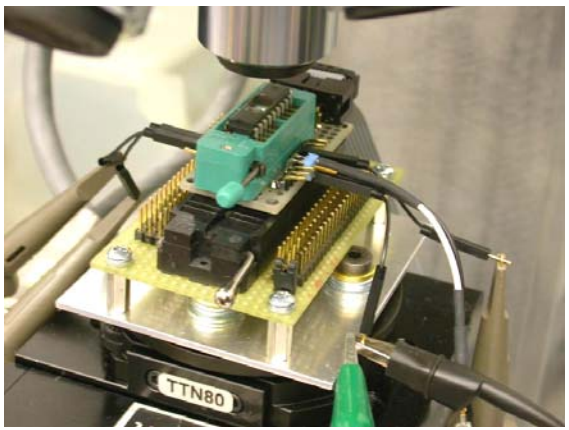


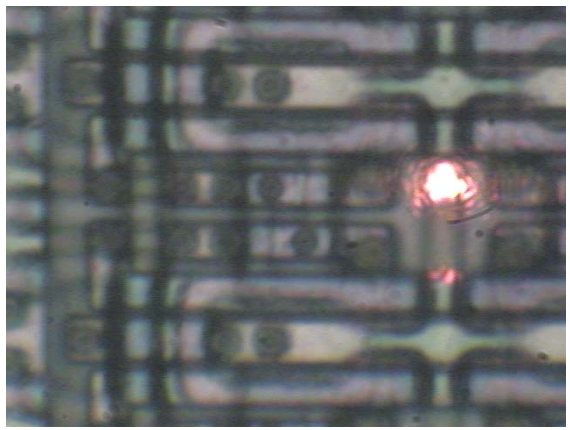


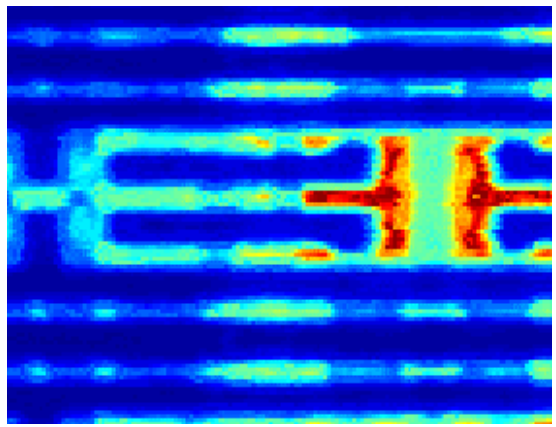
Microchip PIC16F84 microcontroller

Semi-invasive attacks

- Optically enhanced position-locked power analysis
  - Microchip PIC16F84 microcontroller with test program at 4 MHz
  - classic power analysis setup (10 Ω resistor in GND, digital storage oscilloscope) plus laser microscope scanning setup
  - test pattern
    - run the code inside the microcontroller and store the power trace
    - point the laser at a particular transistor and store the power trace
    - compare two traces

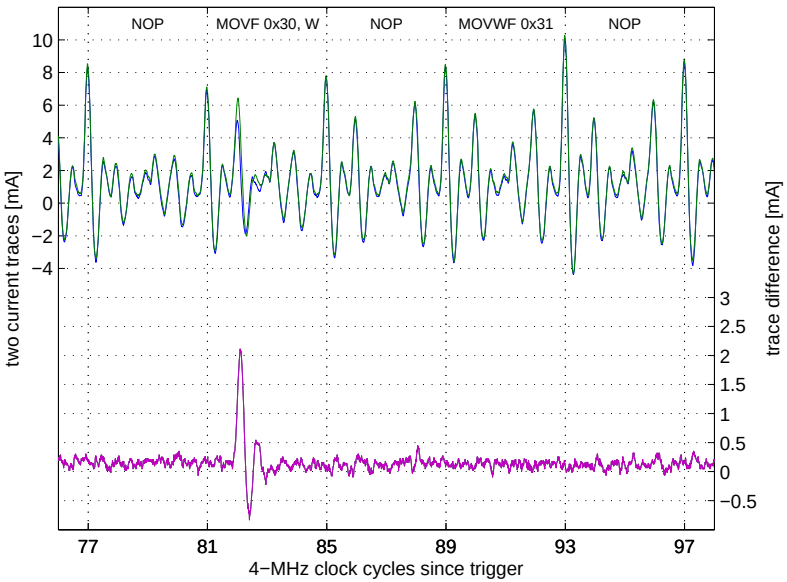


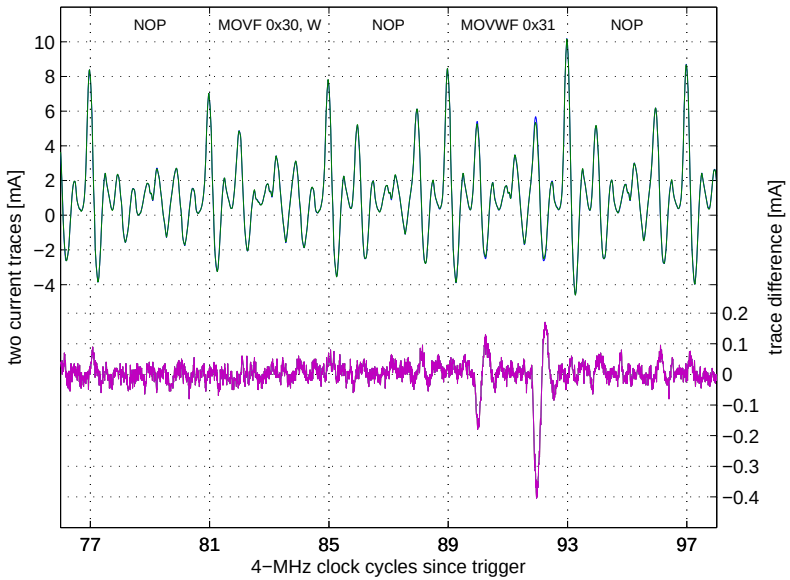




Semi-invasive attacks

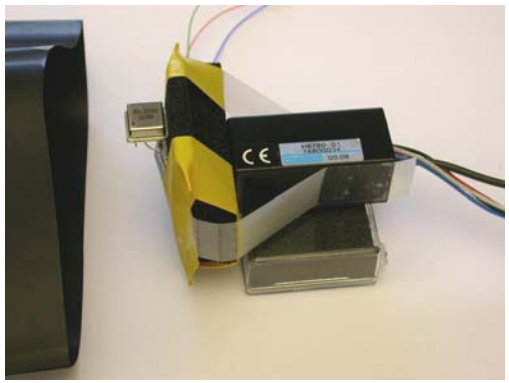
- Optically enhanced position-locked power analysis
  - results for memory read operations: non-destructive analysis of active memory locations (‘0’ and ‘1’)
  - results for memory write operations: non-destructive analysis of active memory locations (‘0→0’, ‘0→1’, ‘1→0’ and ‘1→1’)

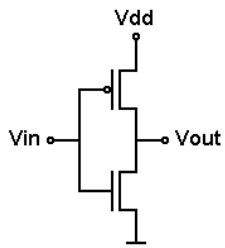


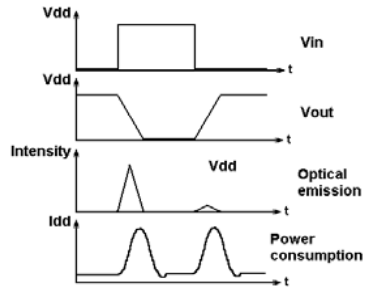


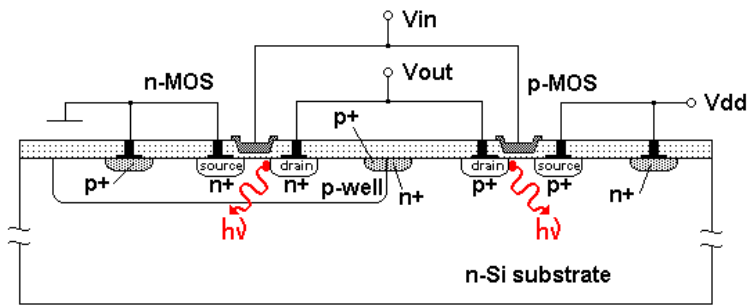
Semi-invasive attacks

- Optical emission analysis
  - transistors emit photons when they switch
  - 10^{-2} to 10^{-4} photons per switch with peak in NIR region (900–1200 nm)
  - optical emission can be detected with photomultipliers and CCD cameras
  - comes from area close to the drain and primarily from the NMOS transistor



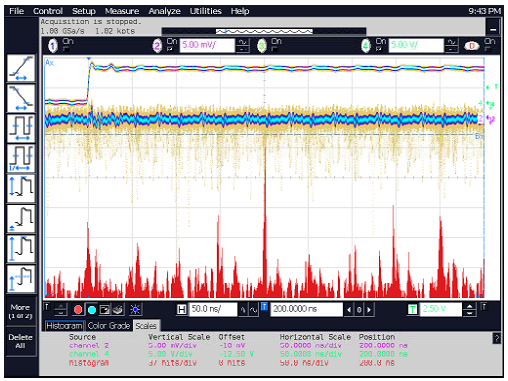


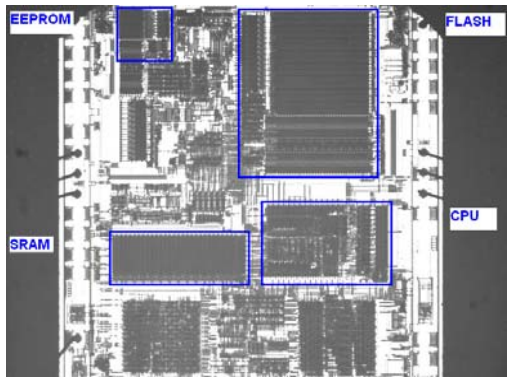


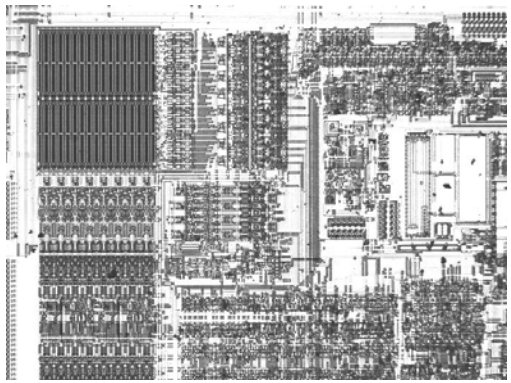


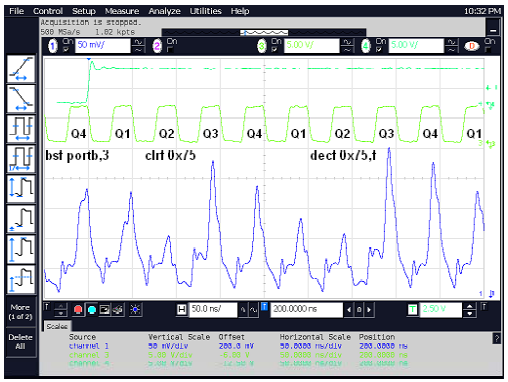
Semi-invasive attacks

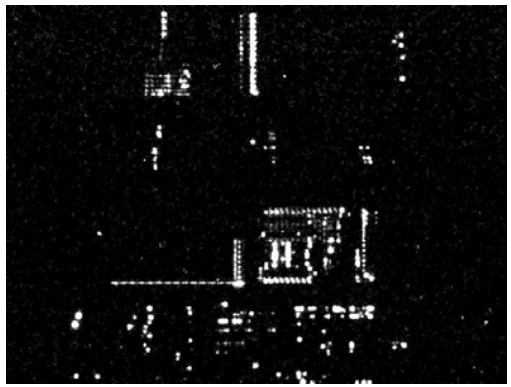
- Optical emission analysis
  - Microchip PIC16F628 microcontroller with test code at 20 MHz
  - PMT vs SPA and CCD camera images
  - takes at least several minutes to acquire the image

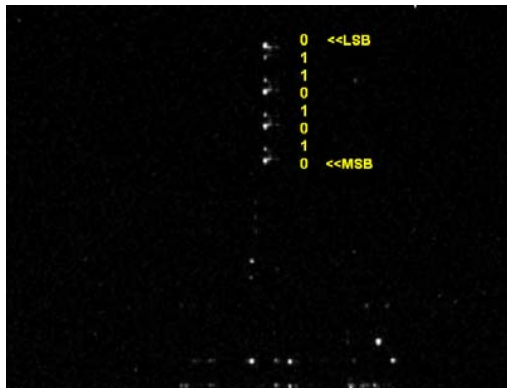












Semi-invasive attacks

- Compared with invasive attacks

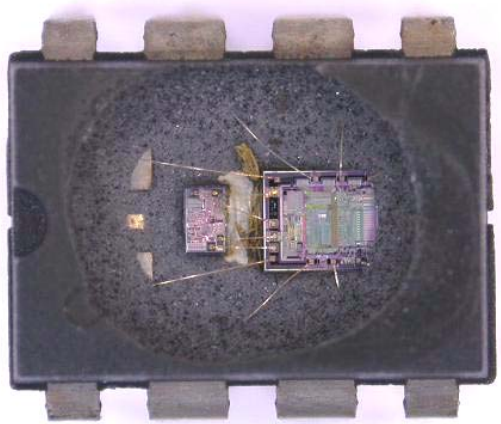
INVASIVE	SEMI-INVASIVE
Microprobing	Laser scanning Optical probing and emission analysis
Chip modification (laser cutter or FIB)	Fault injection
Reverse engineering	Special microscopy
Rear-side approach with a FIB	Infrared techniques

- Compared with non-invasive attacks

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

Defence technologies

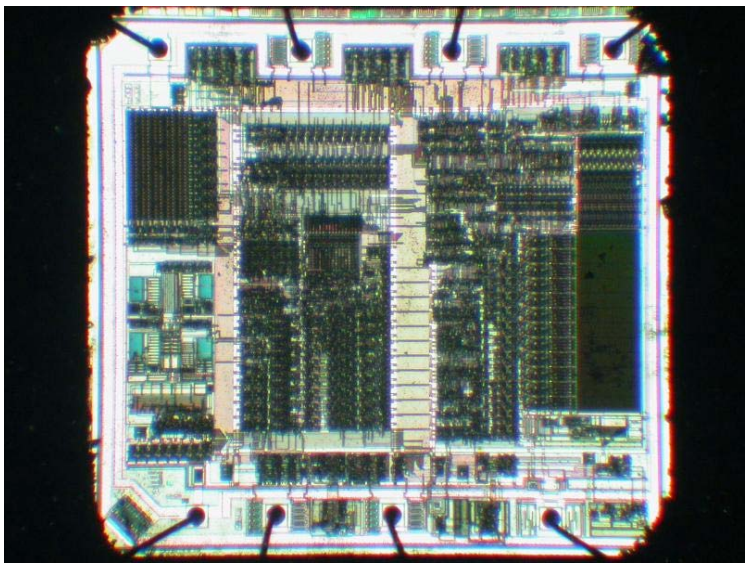
- Tamper protection level MODL
  - hiding
  - restricted access



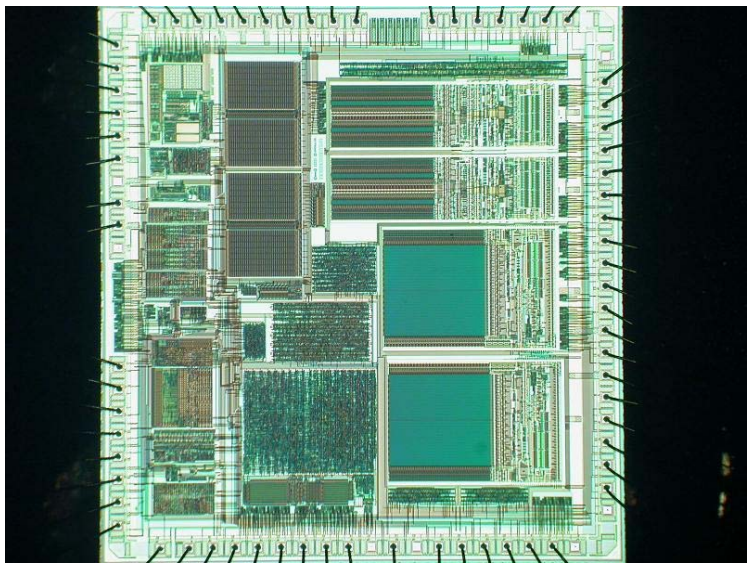
Microchip PIC12CE518 microcontroller

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 encryption keys



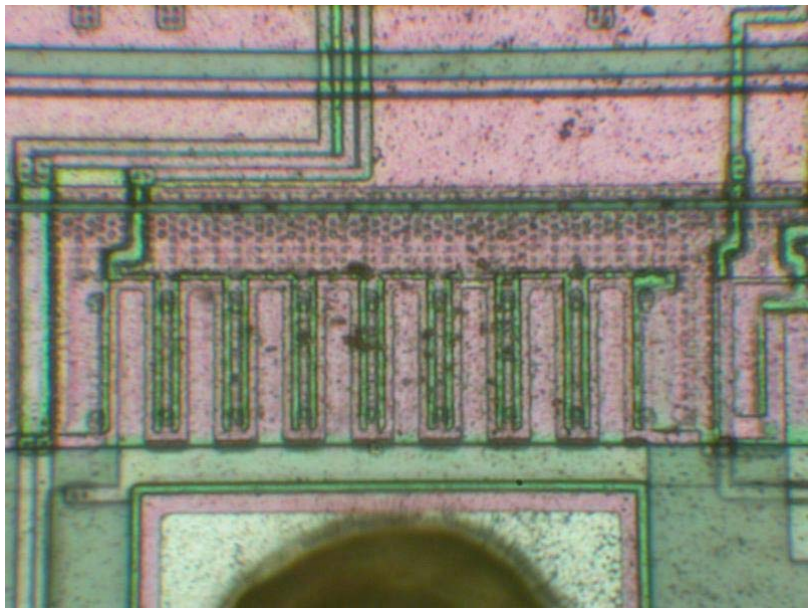
Microchip PIC12C508 microcontroller



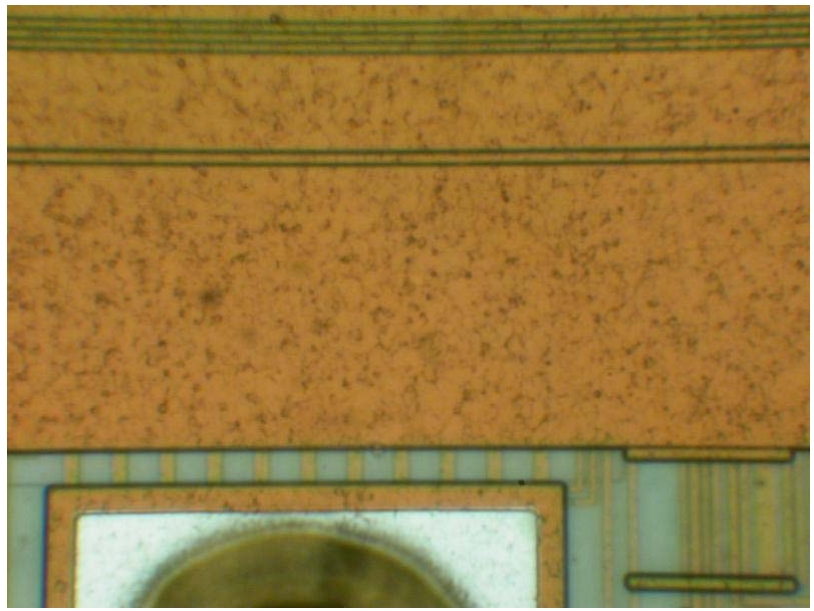
Motorola MC68HC908AZ60A microcontroller

Defence technologies

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



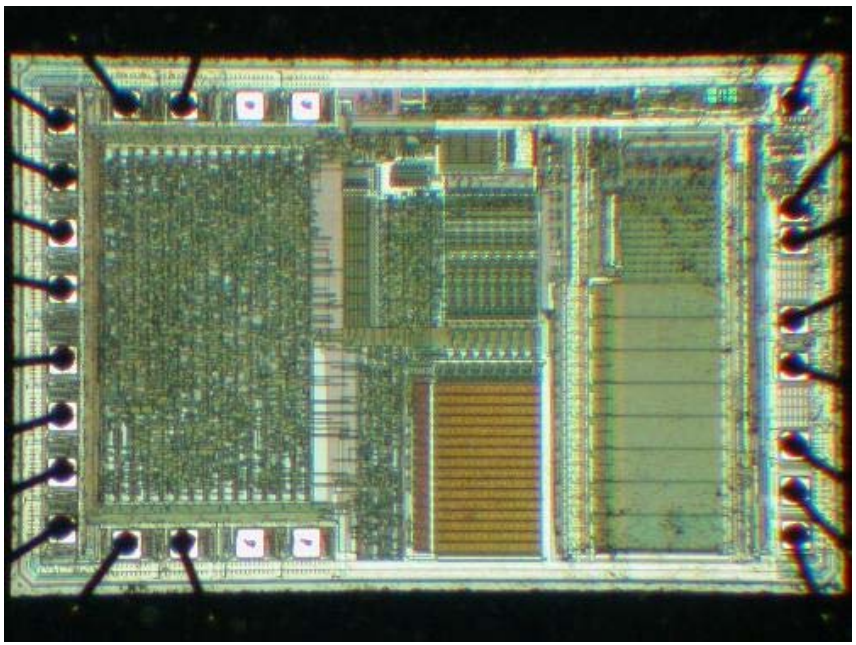
Microchip PIC16F877 microcontroller



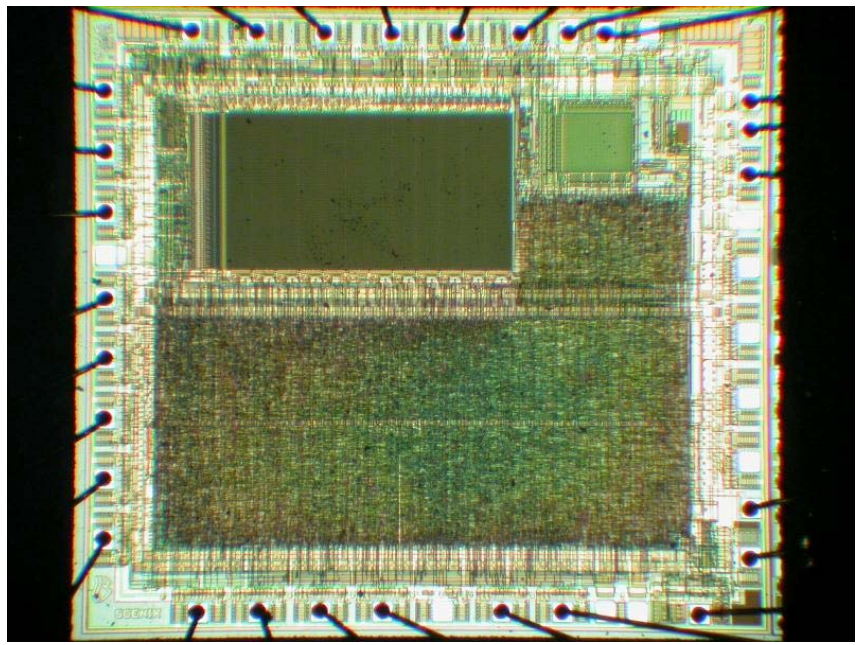
Microchip PIC16F877A microcontroller

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)



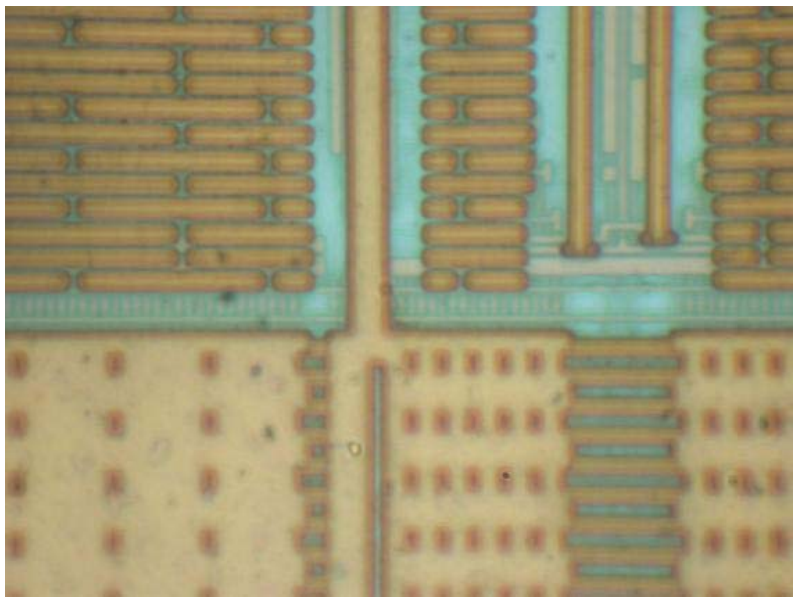
Cypress CY7C63001A microcontroller



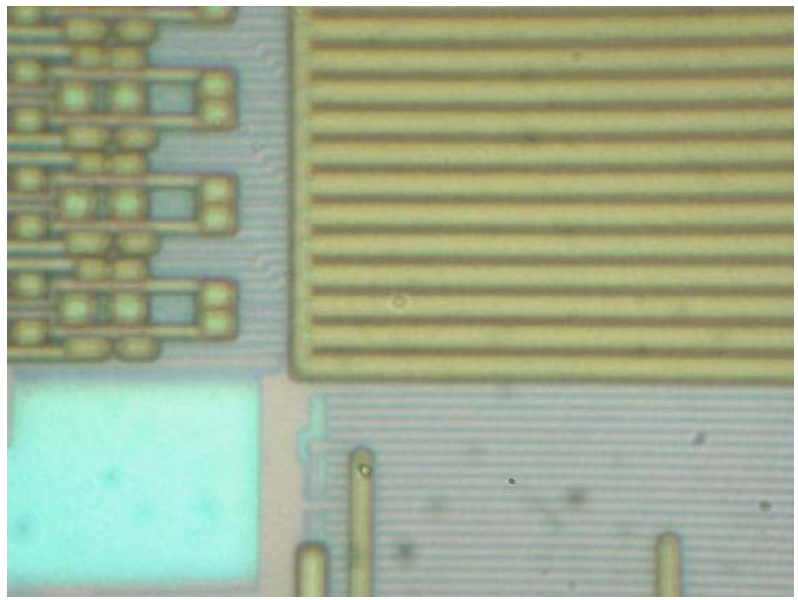
Scenix SX28 microcontroller

Defence technologies

- Tamper protection level MOD
  - fabrication process reduced to under 0.5 μm
  - multiple metal layers obstruct direct observation
  - increased complexity of circuits



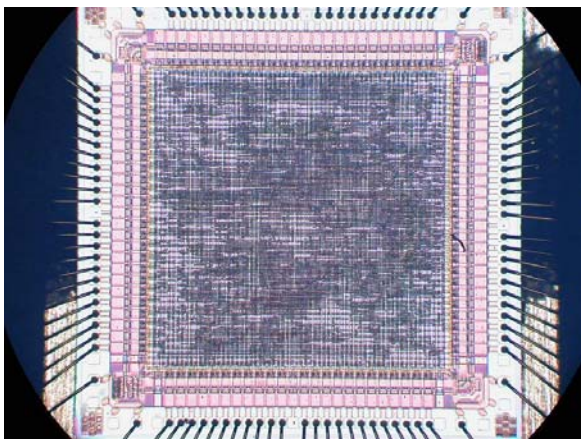
Atmel ATmega16 microcontroller

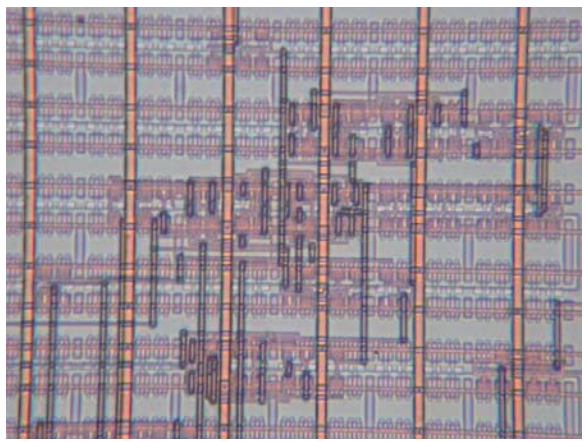


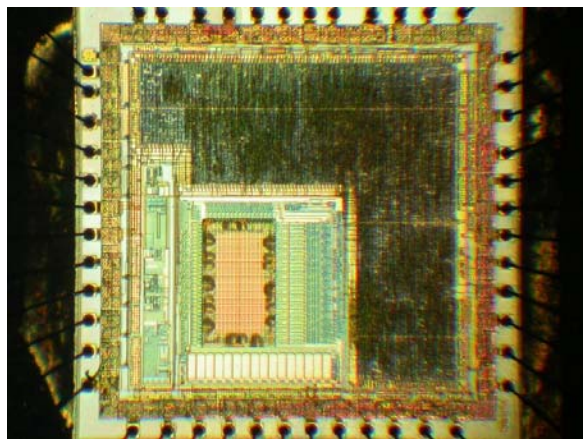
Motorola MC68HC908AP16 microcontroller

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
  - custom-designed ICs
    - reverse engineering is an extremely expensive and long process

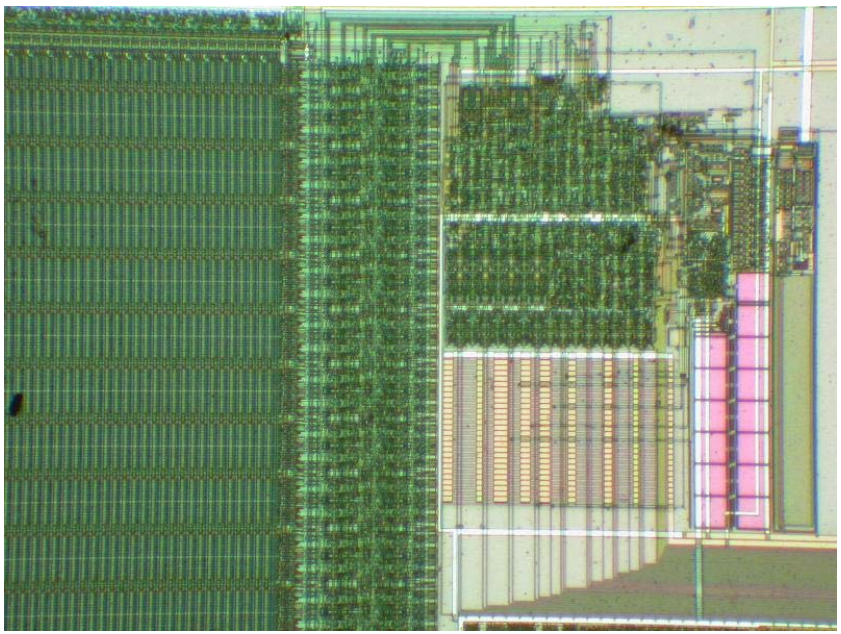






Defence technologies

- Tamper protection level MODH
  - memory management
  - bus encryption – simple algorithms not to slow down the communication

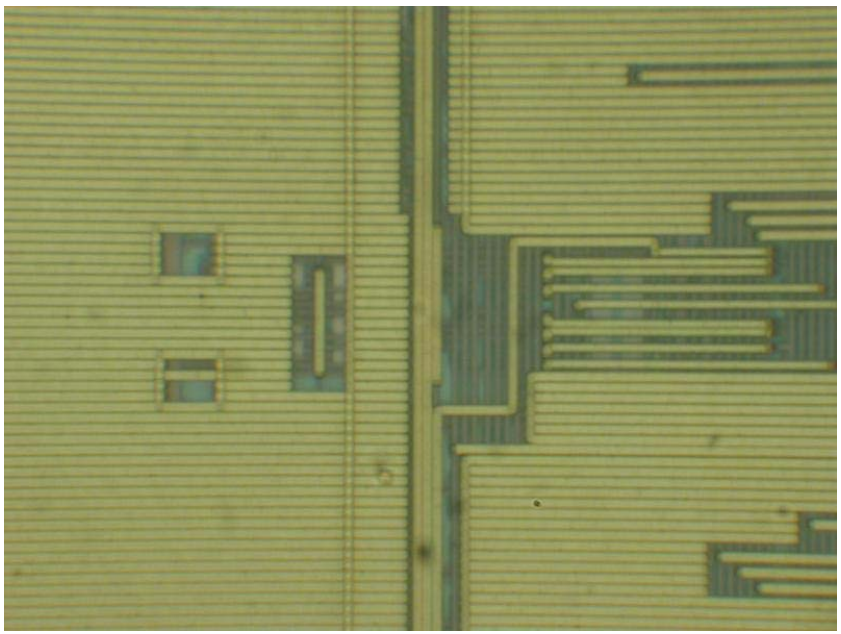


Infineon SLE66 smartcard

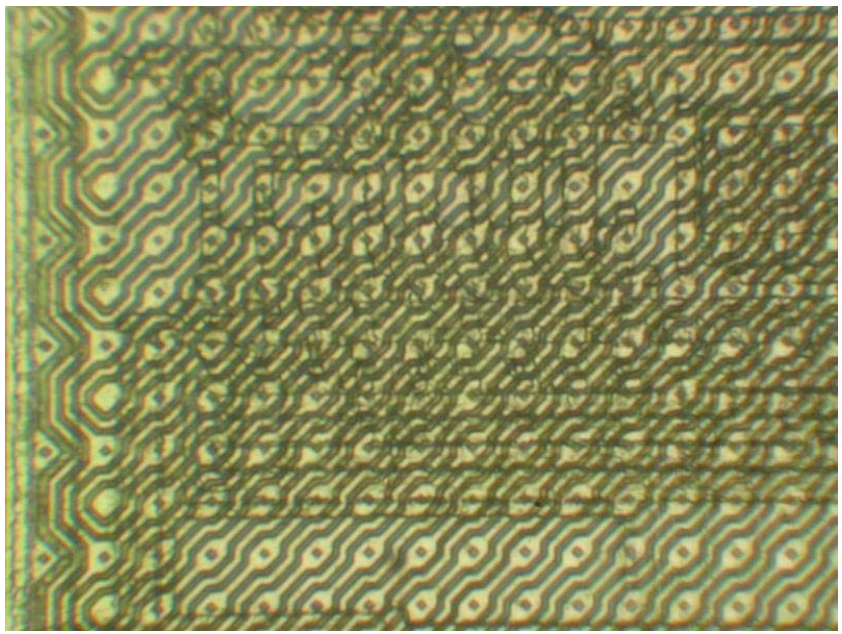
Dallas Semiconductor DS5002FP microcontroller

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 solutions

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

References

- Slides
  - http://www.cl.cam.ac.uk/~sps32/PartII_201109.pdf
- Literature:
  - Ross Anderson's book "Security Engineering"
  - http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.pdf
  - http://www.cl.cam.ac.uk/~sps32/#Publications