Information Security – Theory vs. Reality

0368-4474, Winter 2015-2016

Lecture 7: Fault attacks, Hardware security (1/2)

Lecturer:
Eran Tromer

Fault attacks

Fault attacks on chips: non-nominal channels

- Temperature
- Mechanical stress
- Clock
  - Overlocking, unstable, spikes
- Supply voltage / ground
  - Too low, too high, unstable, spikes
- Electromagnetic
  - Strong electric/magnetic fields
  - Optical
- Chemical
- Inject signals into non-inpu
  - On non-input pins
  - Using probes within circuit

Fault attacks: abusing nominal channels

- Exploits using malformed inputs
  - Buffer overflow, SQL injection, …
- Imperfect behavior and “unlikely” error conditions
  - Rowhammer on DRAM
- Corrupt communication on interfaces with peripherals and network

Fault attacks: trojan horses in the “IT supply chain”

- Hardware design
- Hardware manufacturing
- Software design
- Software manufacturing
- Standards
  - NSA’s Dual_EC_DRBG
- Distribution
- Transportation

Differential Fault Analysis of Arbitrary Decryption

Whiteboard discussion.

[Biham, Shamir, *Differential Fault Analysis of Secret Key Cryptosystems*, CRYPTO 1997 (section 3)]

Fault Analysis of RSA-CRT signatures

Whiteboard discussion:

- Using faulty+correct signature
- Using faulty signature and known message

[DeMillo, Lipton, *On the importance of eliminating errors in cryptographic protocols*, Journal of Cryptology, 2001 (Section 2.2)]

Hardware security (survey and additional vectors)

Including presentation material by
Sergei Skorobogatov, University of Cambridge

Outline

- Introduction
- Attack awareness
- Tamper protection levels
- Attack methods
  - Non-invasive
  - Invasive
  - Semi-invasive
- Protection against attacks
- Conclusions

Physical security

- 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, SIM cards, PayTV smartcards
  - crypto-processors and crypto-modules for encryption
  - mobile phones, game consoles and many other devices
  - product identification for printer ink, perfume etc.

Why do we need hardware security?

- Theft of service
  - attacks on service providers (satellite TV, electronic meters, access cards, software protection dongles)
- Access to information
  - information recovery and extraction
  - gaining trade secrets (IP piracy)
  - ID theft
- Cloning and overbuilding
  - copying for making profit without investment in development
  - low-cost mass production by subcontractors
- Denial of service
  - dishonest competition
  - electronic warfare

Who need secure chips?

- There is growing demand for secure chips
  - car industry, service providers, manufacturers of various devices
  - banking industry and military applications
- Technical progress pushed secure semiconductor chips towards ubiquity
  - consumer electronics (authentication, copy protection)
  - aftermarket control (spare parts, accessories)
  - access control (RF tags, cards, tokens and protection dongles)
  - service control (mobile phones, satellite TV, license dongles)
  - intellectual property (IP) protection (software, algorithms, design)
- Challenges
  - How to design secure system? (hardware security engineering)
  - How to evaluate protection? (estimate cost of breaking)
  - How to find the best solution? (minimum time and money)

How to design a secure system?

- What is the reason to attack your system?
  - attack scenarios and motivations: theft, access, cloning or DoS
- Who is likely to attacks your system?
  - classes of attackers: outsiders, insiders or funded organisations
- What tools would they use for the attacks?
  - attack categories: side-channel, fault, probing, reverse engineering
  - attack methods: non-invasive, invasive, semi-invasive
- How to protect against these attacks?
  - estimate the threat: understand motivation, cost and probability
  - develop adequate protection by locating weak points
  - perform security evaluation
  - choose secure components for your system (blocks and chips)

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

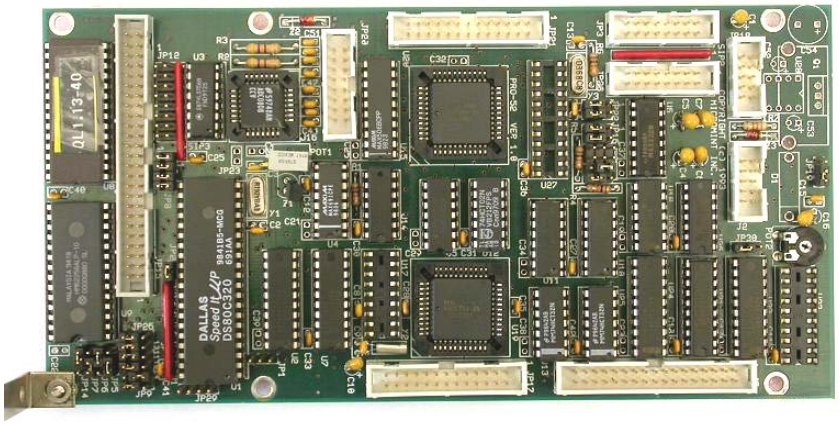
Attack methods

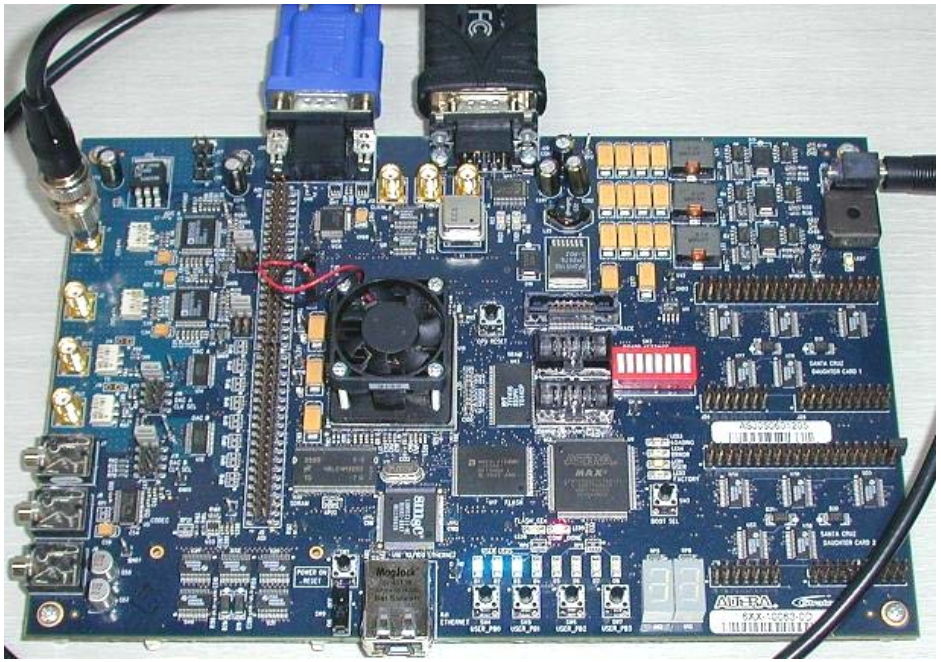
- Non-invasive attacks (low-cost)
  - observe or manipulate with the device without physical harm to it
  - require only moderately sophisticated equipment and knowledge to implement
- Invasive attacks (expensive)
  - almost unlimited capabilities to extract information from chips and understand their functionality
  - normally require expensive equipment, knowledgeable attackers and time
- Semi-invasive attacks (affordable)
  - 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

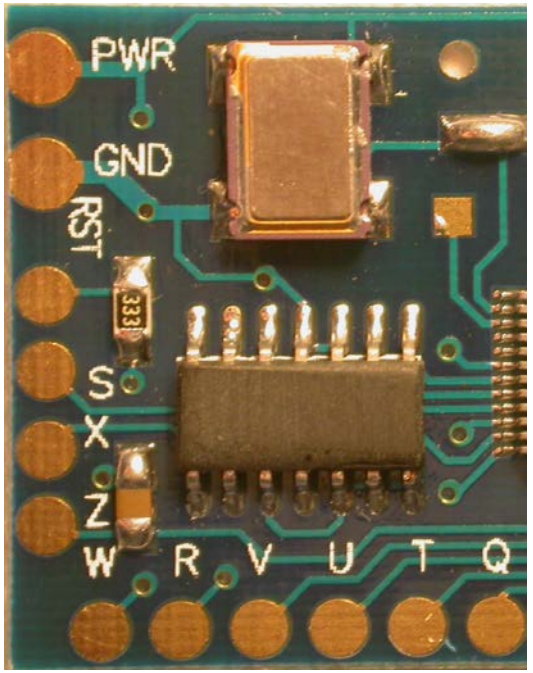
- Level ZERO (no special protection)
  - microcontroller or FPGA with external ROM
  - no special security features are used. All parts have free access and can be easily investigated
  - very low cost, attack time: minutes to hours





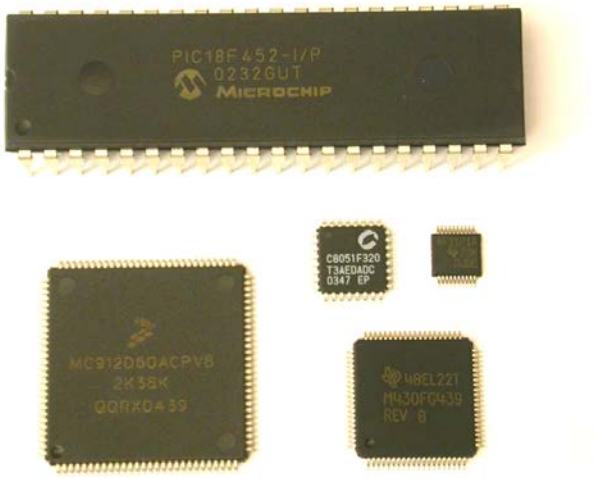
Tamper protection levels

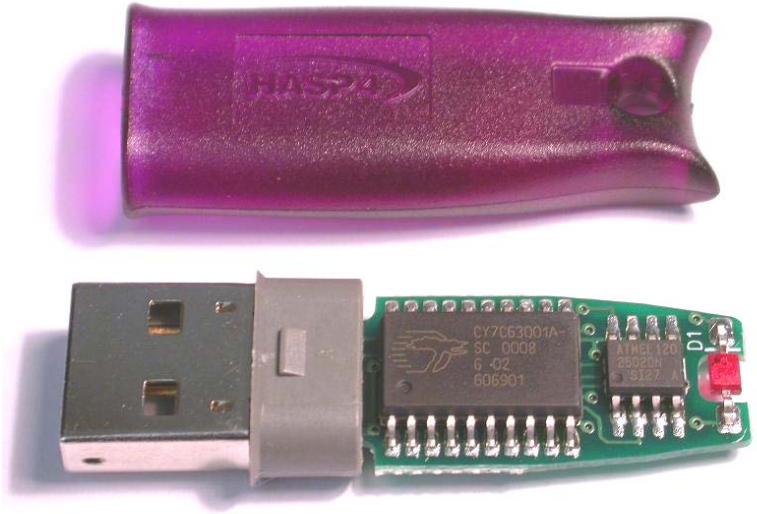
- Level LOW
  - microcontrollers with proprietary access algorithm, remarked ICs
  - some security features are used but they can be relatively easy defeated with minimum tools required
  - low cost, attack time: hours to days



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



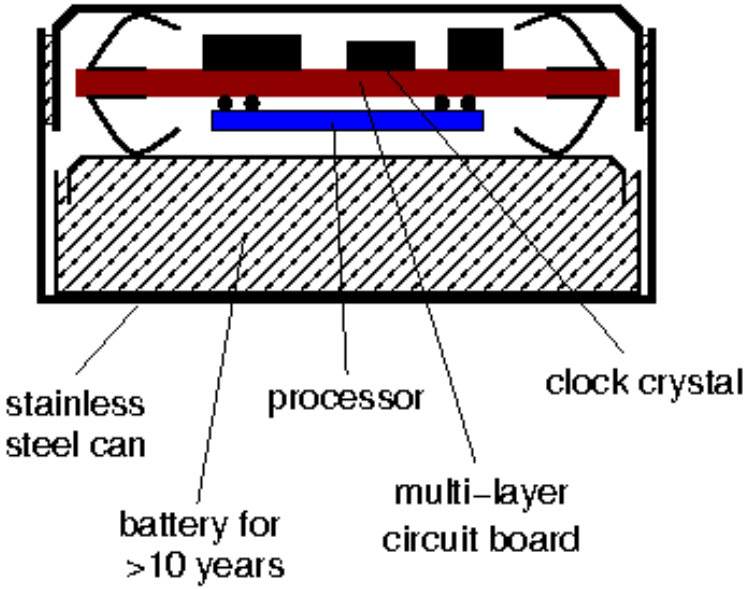


Tamper protection levels

- 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

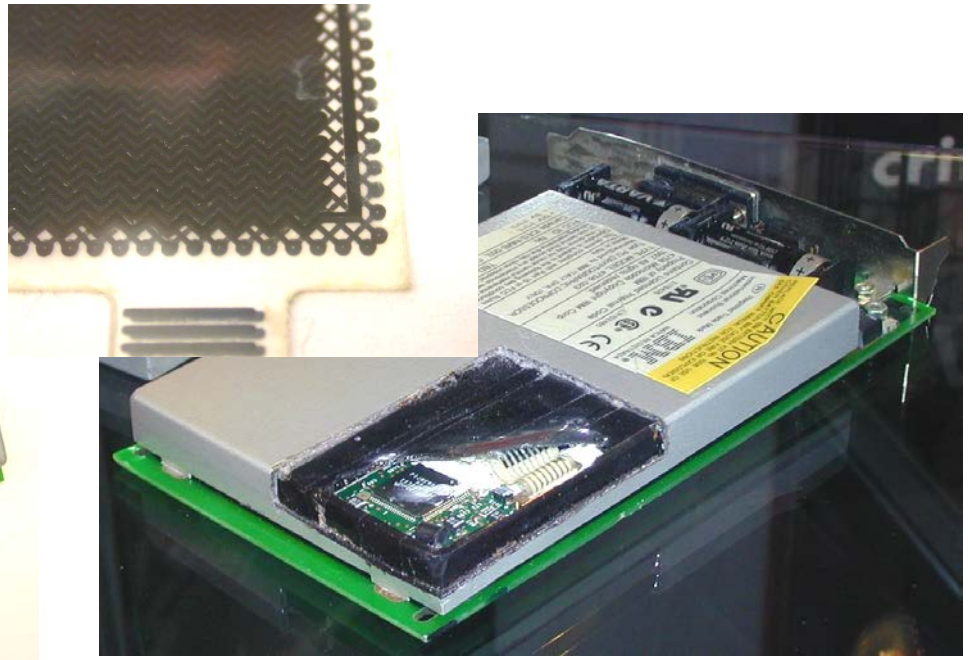
- Level MODH
  - secure i-Buttons, secure FPGAs, high-end smartcards, ASICs, custom secure ICs
  - special attention is paid to design of the security protection; equipment is available but is expensive to buy and operate
  - very high cost, attack time: months to years



Picture courtesy of Dr Markus Kuhn

Tamper protection levels

- Level HIGH
  - Primary example: Hardware Security Modules (HSMs)
  - military, banks, ATM, certificate authorities
  - 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-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: passive and active
  - side-channel attacks: timing, power, electromagnetic, acoustic, thermal, …
  - data remanence
  - fault injection: glitching, bumping
  - brute forcing

Non-invasive attacks: side-channel

(discussed previously)

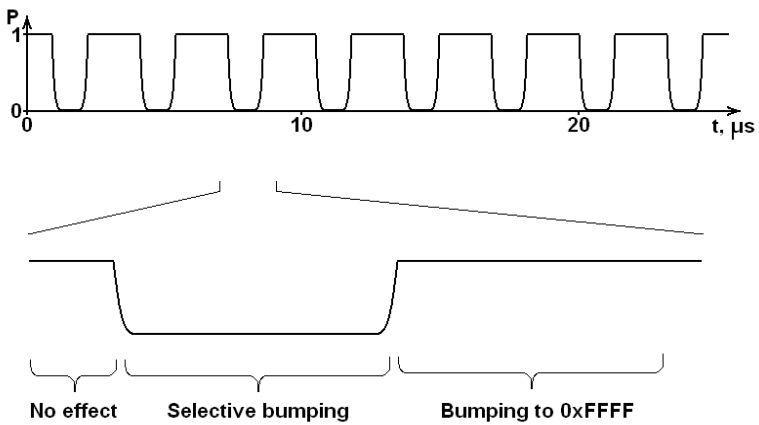
Non-invasive attacks: fault injection

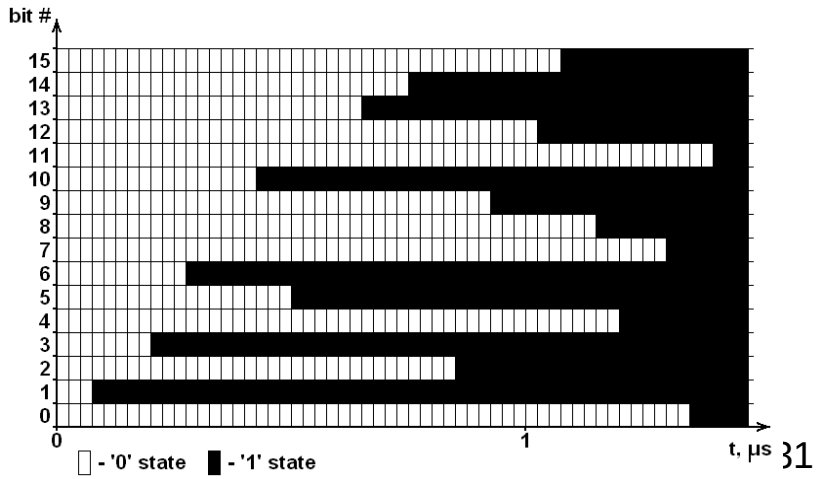
- Glitch attacks
  - clock glitches
  - power supply glitches
  - data corruption
- Security fuse verification in the Mask ROM bootloader of the Motorola MC68HC05B6 microcontroller
  - double frequency clock glitch causes incorrect instruction fetch
  - low-voltage power glitch results in corrupted EEPROM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

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

Non-invasive attacks: fault injection

- Bumping and selective bumping attacks
  - aimed at internal integrity check procedure on a chip (verification and authentication using encryption or hash functions)
  - aimed at blocks of data down to bus width or at individual bits within the bus
- Power supply glitching attack on secure microcontroller
  - exhaustive search: 2^{127} attempts per 128-bit AES key → >trillion years
  - bumping: 2^{15} attempts per 16-bit word, 100ms cycle, 8 hours for AES key
  - selective bumping: 2^{7} attempts per 16-bit word, 2 minutes for AES key





Non-invasive attacks: brute forcing

- 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
  - applying random signals and commands to find hidden functionality
- Modern chips deter most brute force attacks
  - longer keys make searching infeasible
  - moving from 8-bit base to 32-bit base means longer search
  - CPLDs, FPGAs and ASICs became too complex to analyse
  - too large search field for finding hidden functionality

Non-invasive attacks: data remanence

(discussed in previous lecture)

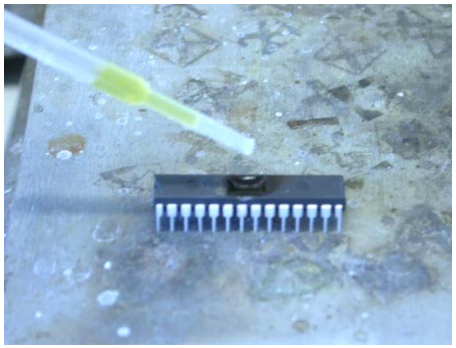
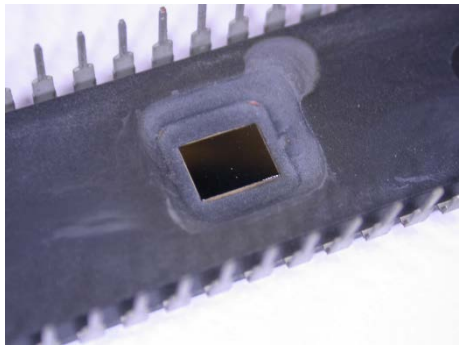
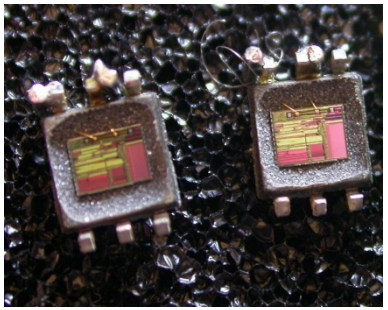
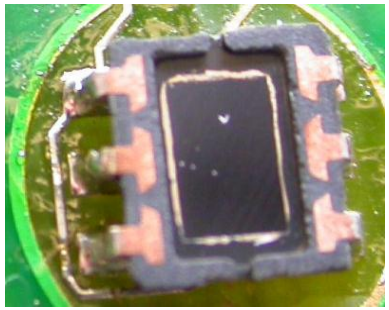
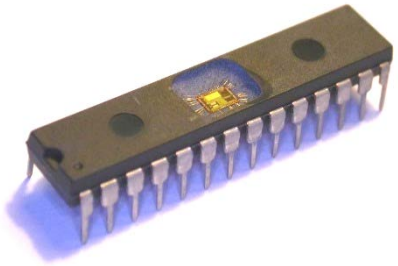
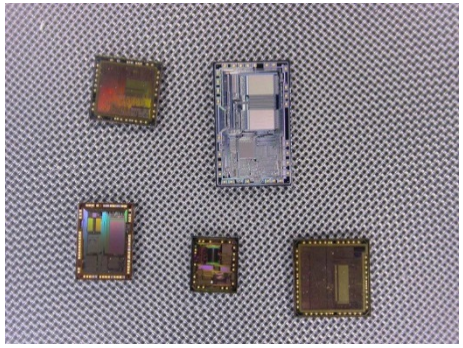
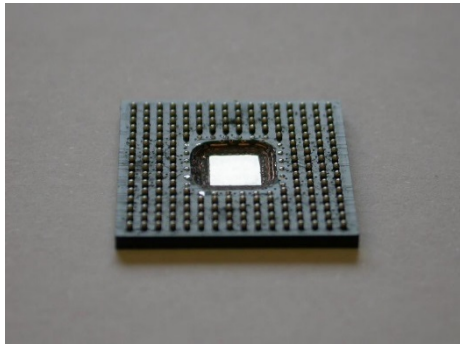
Invasive attacks

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
  - scanning electron microscope and focused ion beam workstation
- Types of invasive attacks: passive and active
  - decapsulation, optical imaging, reverse engineering
  - microprobing and internal fault injection
  - chip modification

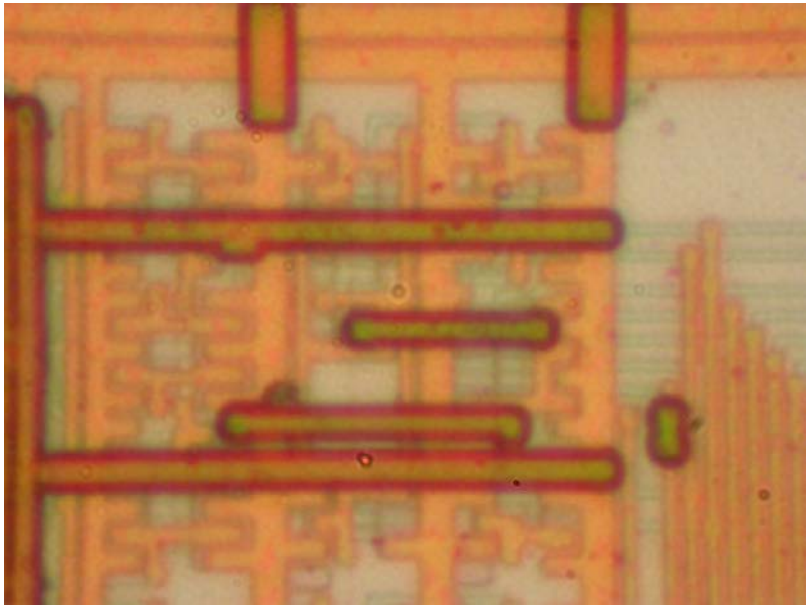
Invasive attacks: sample preparation

- 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 from rear side
- Challenging process for small and BGA packages

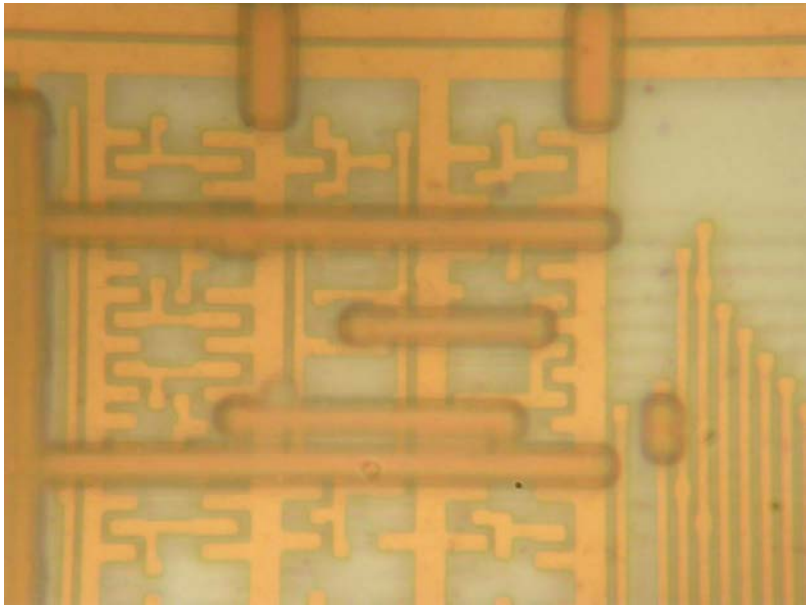








Invasive attacks: imaging

- 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 ($n = 1.5$)



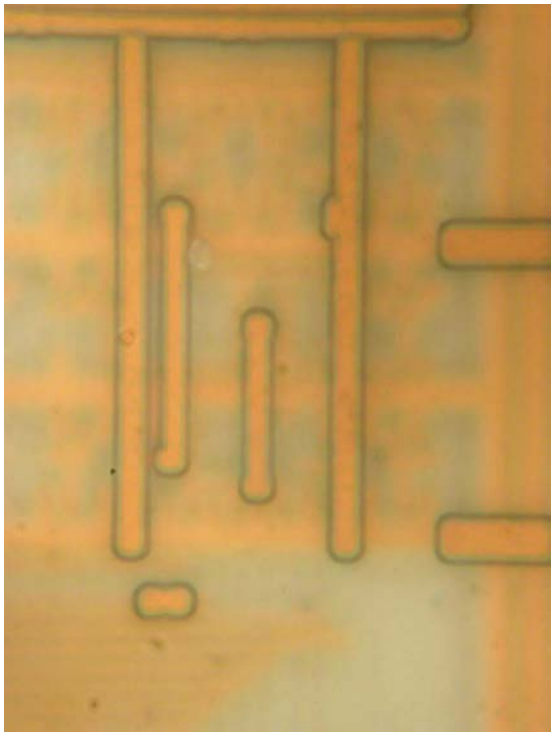
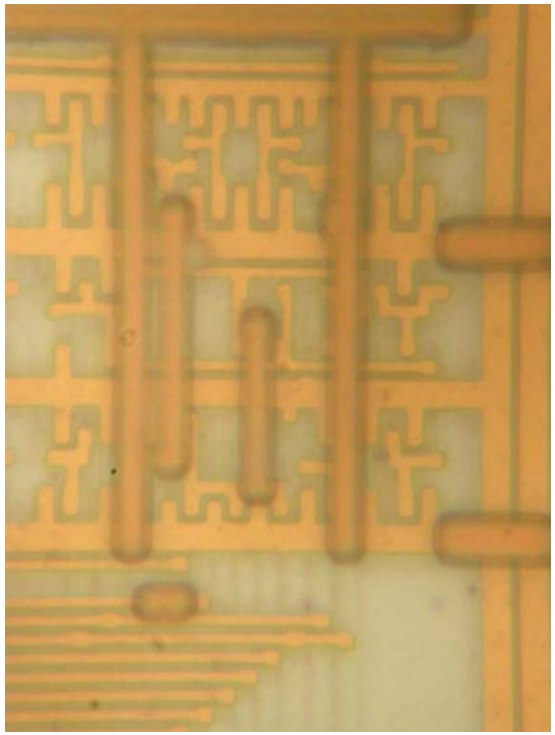
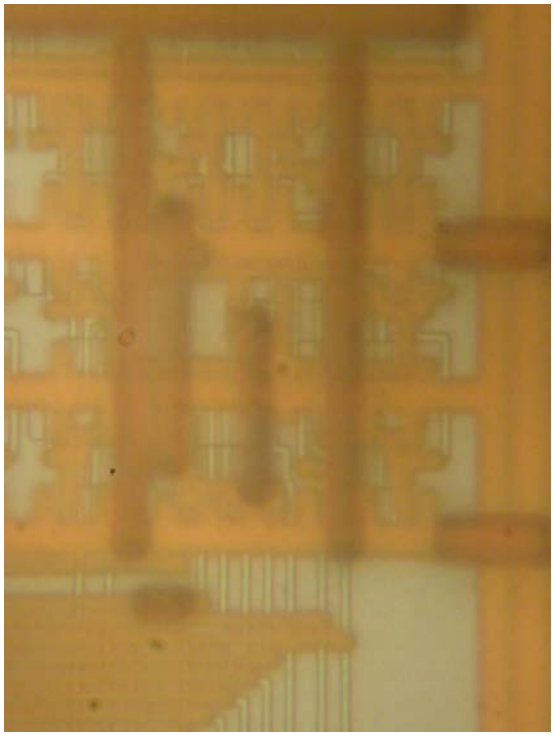
Bausch&Lomb MicroZoom, 50×2×, NA = 0.45



Leitz Ergolux AMC, 100×, NA = 0.9

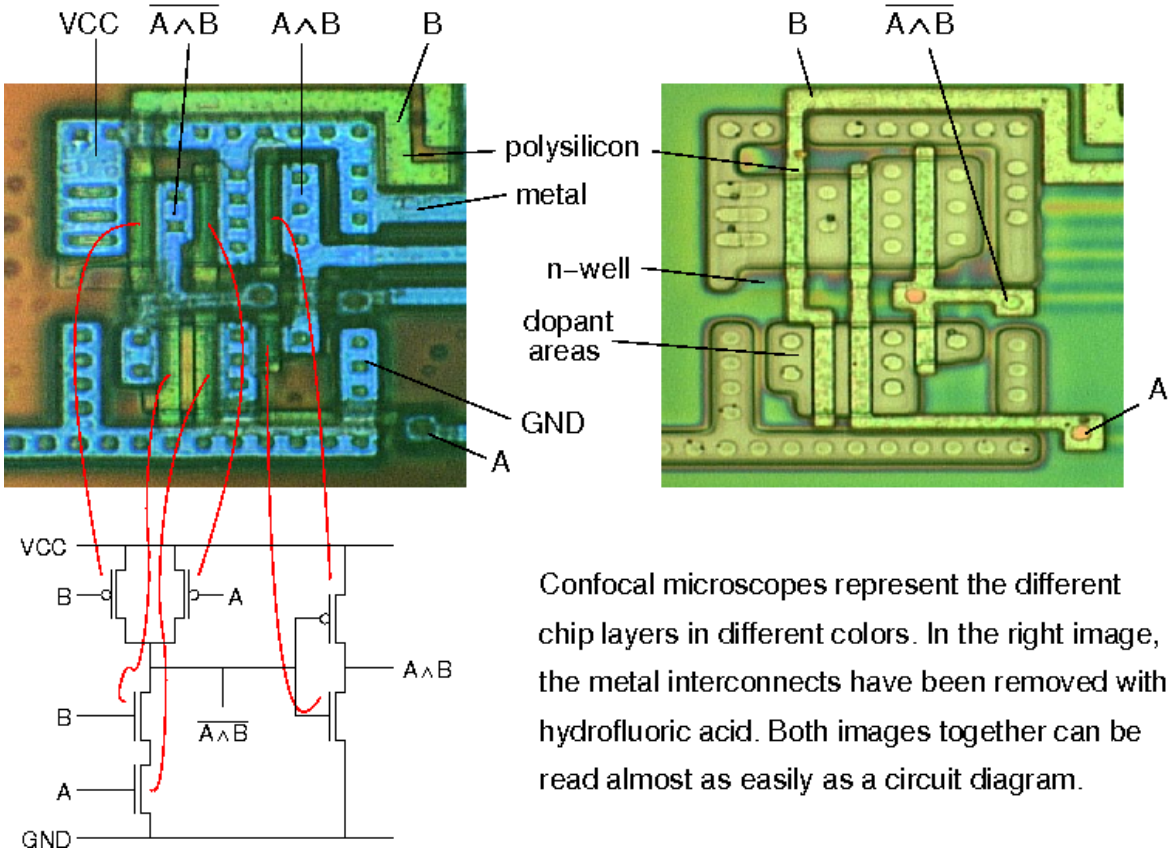
Invasive attacks: imaging

- Optical imaging
  - image quality depends on microscope optics
    - depth of focus helps in separating the layers
    - geometric distortions pose problem for later post-processing

Invasive attacks: reverse engineering

- 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

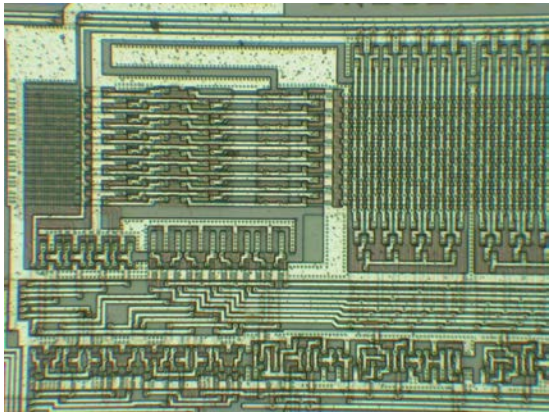


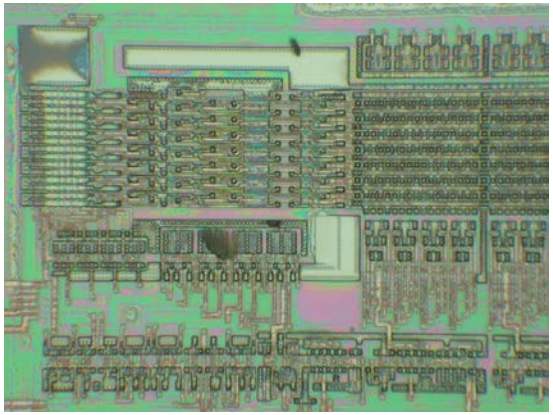
Confocal microscopes represent the different chip layers in different colors. In the right image, the metal interconnects have been removed with hydrofluoric acid. Both images together can be read almost as easily as a circuit diagram.

Picture courtesy of Dr Markus Kuhn

Invasive attacks: reverse engineering

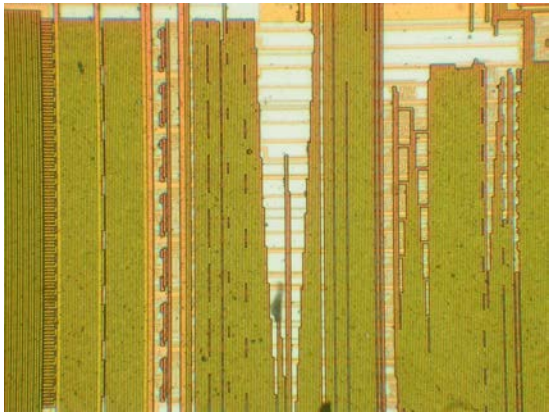
- Removing top metal layer using wet chemical etching
  - good uniformity over the surface, but works reliably only for chips fabricated with 0.8 µm or larger process (without polished layers)

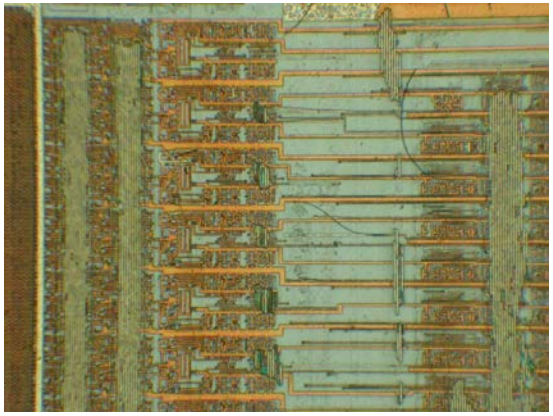




Motorola MC68HC705C9A microcontroller

1.0 µm



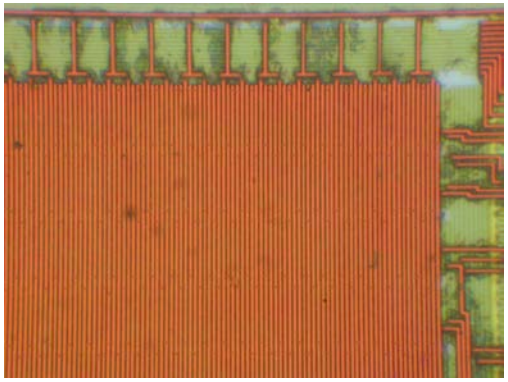


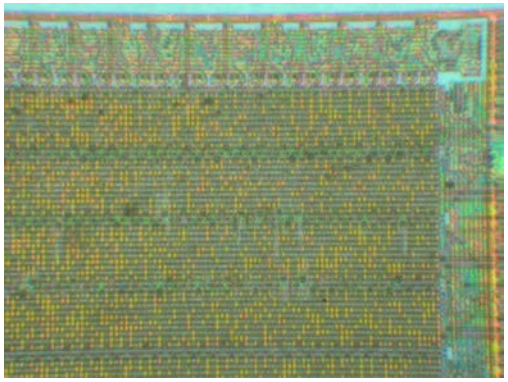
Microchip PIC16F76 microcontroller

0.5 µm

Invasive attacks: reverse engineering

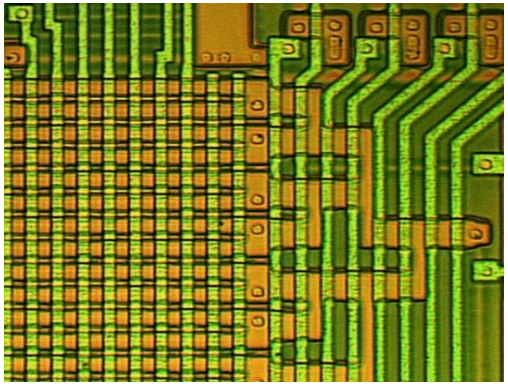
- Memory extraction from Mask ROMs
  - removing top metal layers for direct optical observation of data in NOR ROMs (bits programmed by presence of transistors)
  - not suitable for VTROM (ion implanted) used in smartcards – selective (dash) etchants are required to expose the ROM bits

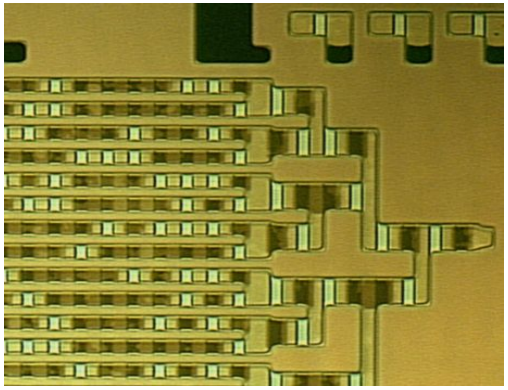




NEC μPD78F9116 microcontroller

0.35 μm





Motorola MC68HC05SC27 smartcard

1.0 μm

Picture courtesy of Dr Markus Kuhn