UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Lecture 7 - Physical Attacks and Protections

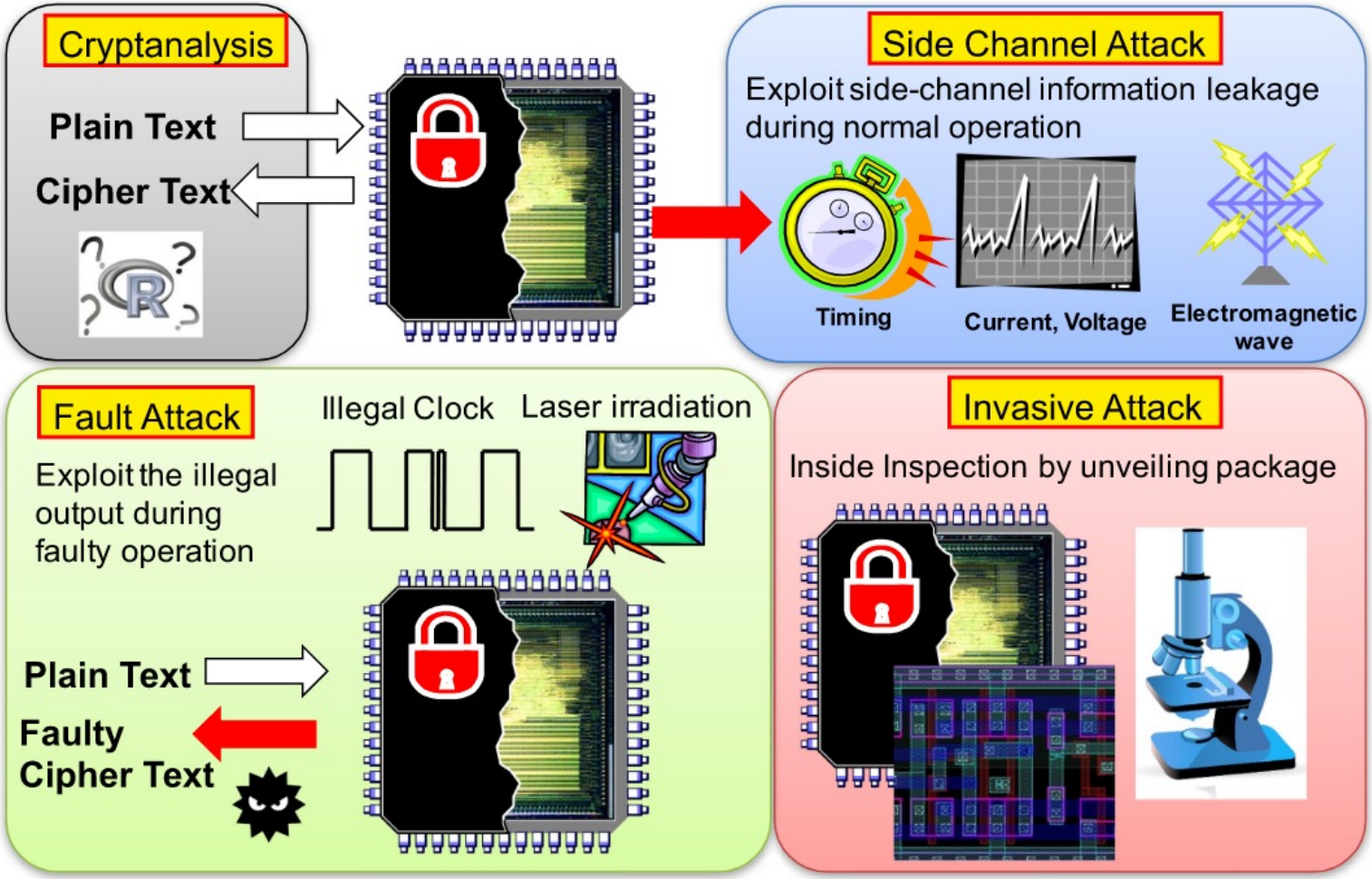
Prof. Esposito Christian

::.. Summary

- Tampering IoT Nodes – Part 3
  - Invasive, Non-invasive, Semi-invasive Attacks
- Protecting IoT Nodes
  - Tamper Resistance

Physical Attacks

::.. Physical Attacks to Hardware

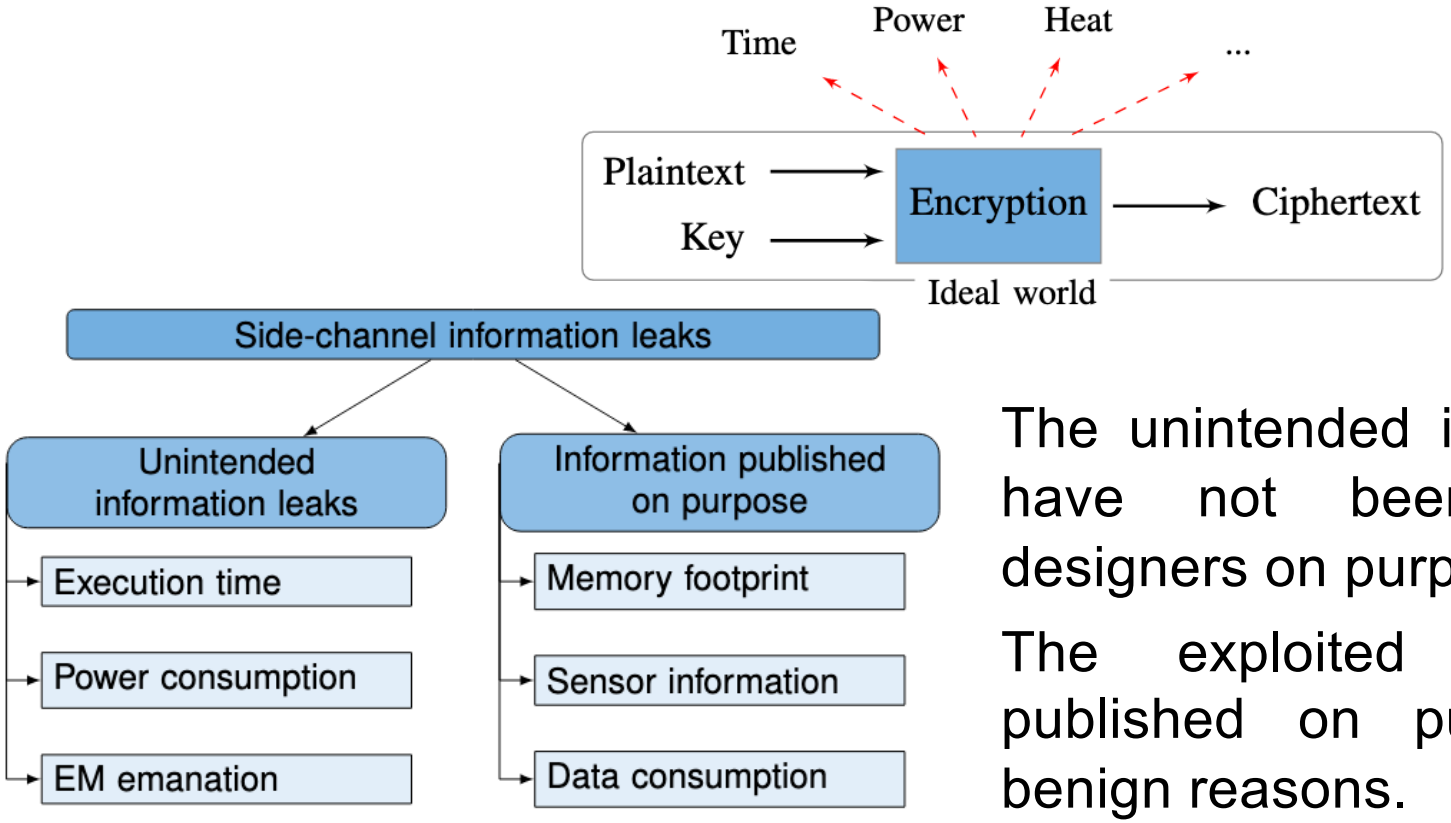


::.. Non Invasive Attacks

- 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 and emission analysis
  - data remanence
  - fault injection: glitching, bumping
  - brute forcing

::.. Side Channel Attack (1/11)

A side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs).

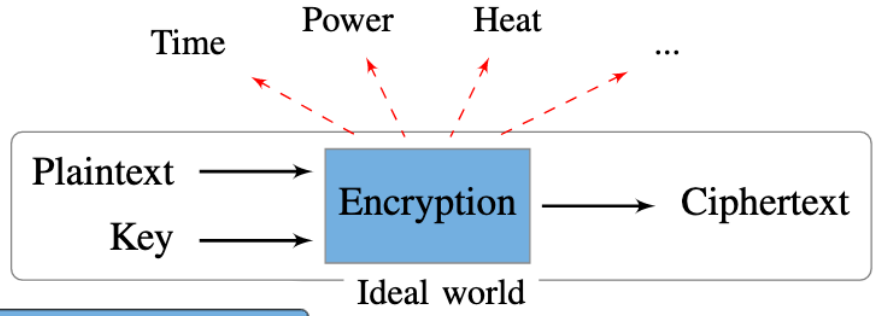


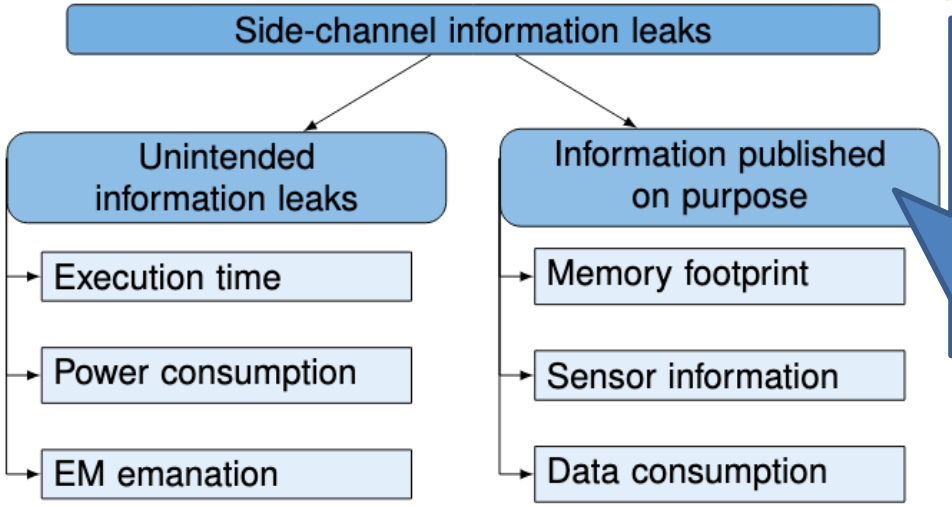
The unintended information leaks have not been planned by designers on purpose.

The exploited information is published on purpose and for benign reasons.

::.. Side Channel Attack (1/11)

A side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs).





The memory footprint of an application as well as the data-usage statistics that keep track of the amount of incoming and outgoing network traffic may allow to infer a user's visited websites.

published on purpose and for benign reasons.

::.. Side Channel Attack (2/11)

- 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, cache memory usage, non-fixed time operations
- 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; very effective against many cryptographic algorithms and password verification schemes
  - some knowledge in electrical engineering and digital signal processing is required
  - two basic methods: simple (SPA) and differential (DPA)
- Electro-magnetic analysis (EMA): measuring emission
  - similar to power analysis, but instead of resistor, a small magnetic coil is used allowing precise positioning over the chip

::.. Side Channel Attack (3/11)

Each operation has a specific execution time within a given architecture, and by measuring the time it is possible to determine what kind of operation has been executed and how many times. Usually consumed time depends on input data, crypt keys, and modulo in cryptosystems.

During the attack, the adversary keeps the input, output, and consumed time, and checks the correlation between time measurements of guess key or input and empirical result (often statistically).

It is an extremely simple attack and also extremely powerful because isolation doesn't help:

- Victim could be remote;
- Victim could be inside its own virtual machine;
- Keys could be in tamper-proof storage or smartcard.

::.. Side Channel Attack (4/11)

Timing attack is often used to compromise public-key cryptosystem such as RSA; therefore, inappropriate usage of it revels its secret key easily.

Timing attacks reveal key length, key values, plaintext, etc…

RSA review

- Multiple prime RSA key generating algorithm

  1. Select two primes: ***p*** and ***q***;

  2. Calculate ***n*** = ***p*** * ***q***, which is the modulus for the public key and the private keys;

  3. Calculate ***φ(n)*** = (***p***-1) * (***q***-1), which is the totient of the positive integer n, i.e., the number of positive integers smaller than n which are coprime to n;

  4. Choose ***e*** such that 1 < ***e*** < ***φ(n)***, and ***e*** is co-prime to ***φ(n)*** by sharing no factors other than 1 or gcd(***e***,***φ(n)***) = 1;

  5. Calculate ***d*** = e^{-1} mod ***φ(n)***, so as to to satisfy the congruence relation ***d*** * ***e*** = ***1*** mod ***φ(n)***;
  6. Public Key = (***e***,***n***) and Private key = (***d***);

- Encryption: $c = m^e \bmod n$ and Decryption: $m = c^d \bmod n$

::.. Side Channel Attack (5/11)

The way of attacks depend on the details of modular exponentiation.

For efficiency, modular exponentiation is done via multiple methods, such as simple multiplication:

- the modular exponentiation is done by multiplying the number as many as the values of exponent such as 2^13 = 2 * 2 * 2 * 2 * 2 * 2* …. *2. Therefore, the execution time is direct proportional to the exponent value (key value).

An attacker eavesdrops the decryption operation where he gets a plaintext and its computation time (the decryption key is 13 which is hidden from the attacker).

- He guesses the key is 12. He decrypts with the guess key and it returns small computation time;
- Then, he guesses the key is 14 and retuned computation time is greater than empirical data;
- Now, he knows the key is between 12 and 14.

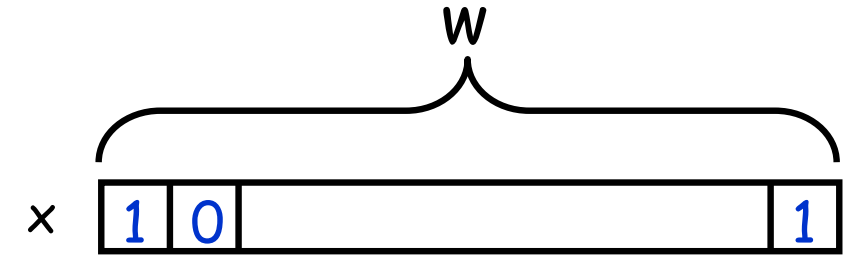
::.. Side Channel Attack (6/11)

- the modular exponentiation can be done with exponentiating by squaring is a general method for fast computation of large positive integer powers of a number:

$$x^n = \begin{cases} x\,(x^2)^{\frac{n-1}{2}}, & \text{if } n \text{ is odd} \\ (x^2)^{\frac{n}{2}}, & \text{if } n \text{ is even.} \end{cases}$$

The number of loops is proportional to its key bit length.

Let $s_0 = 1$.
For $k = 0$ upto $w - 1$:
  If (bit k of x) is 1 then
    Let $R_k = (s_k \cdot y) \bmod n$.
  Else
    Let $R_k = s_k$.
  Let $s_{k+1} = R_k^2 \bmod n$.
EndFor.
Return (R_{w-1}).



::.. Side Channel Attack (6/11)

- the modular exponentiation can be done with exponentiating by squaring is a general method for fast computation of large positive integer powers of a number:

$$x^n = \begin{cases} x\,(x^2)^{\frac{n-1}{2}}, & \text{if } n \text{ is odd} \\ (x^2)^{\frac{n}{2}}, & \text{if } n \text{ is even.} \end{cases}$$

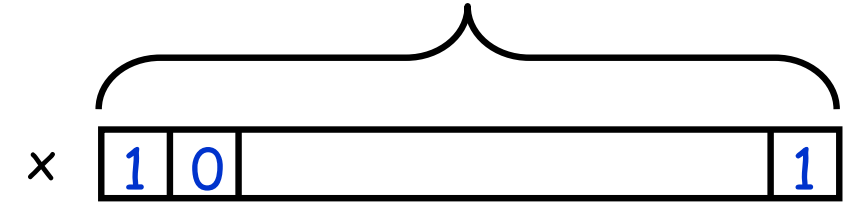
The number of loops is proportional to its key bit length.

```
Let s_0 = 1.
For k = 0 upto w − 1.
  If (bit k of x) is 1 then
    Let R_k = (s_k · y) mod n.
  Else
    Let R_k = s_k.
  Let s_{k+1} = R_k^2 mod n.
EndFor.
Return (R_{w−1}).
```

Whether iteration takes a long time depends on the k^{th} bit of secret exponent

This takes a while to compute

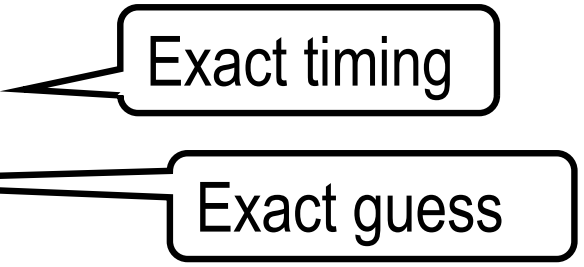
This is instantaneous



::.. Side Channel Attack (7/11)

The attack proposed by Kocher is based on different timing given operands:

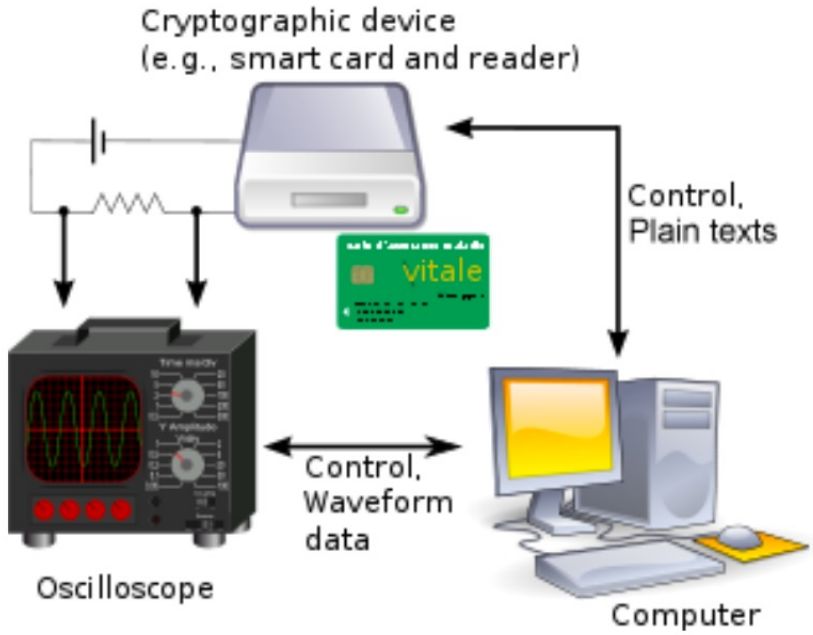
- Given that we know the first k-1 bits of x;
- Given a guess for the k^{th} bit of x;
- Time of remaining bits independent



- First, the attacker wants to know the first bit of the secret key where he has a target plaintext and knows its consumed time;
- He decrypts the plaintext with 1111;
- Next he decrypts the plaintext with 0111;
- Then he creates two graphs for each pair of consumed times;
- Then he finds the strong correlation for 0111 especially at the last step. Thus the first bit may be 0.
- He continues this procedure to the next bit and so on;
- He can efficiently recover low-order bits when enough high-order bits are known because of error correlation property.

::.. Side Channel Attack (7/11)

The simple power analysis (SPA) attacks rely on the interpretation of power traces in order to reveal, for example, the sequence of executed instructions, which allows to break implementations where the executed instructions depend on secret data.



The power consumption of a CMOS circuits is made up of two components:

- Static power is due to the leakage current of transistors and dependent on the design of the circuit.
- Dynamic power is due to the switching of transistors and dependent on the data being processed and the operation being done.

::.. Side Channel Attack (8/11)

The SPA can be used to attack the RSA algorithm: the attacker's objective is to extract the private key d, which is used during the decryption.

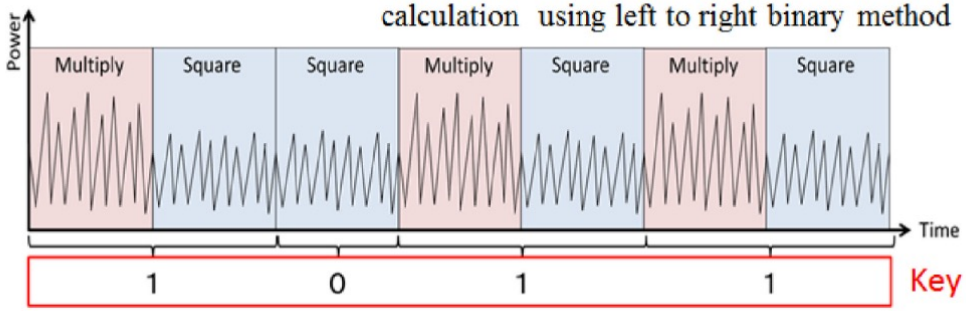
$$C = P^e \bmod N$$
$$P = C^d \bmod N$$

C: Cipher Text
P: Plain Text
e: Public Key
d: Private Key
N: modulo

(a) RSA crypto algorithm

```
input : X, N, d = (d_{k-1},d_{k-2},.....,d_0)
output: Z = X^d mod N
Z←1;
For i = k − 1 down to 0 do
   Z ←Z× Z mod N;     //Square
      if (d_i = 1) then
      Z←Z× X mod N;  //Multiply
   end
end
return Z;
```

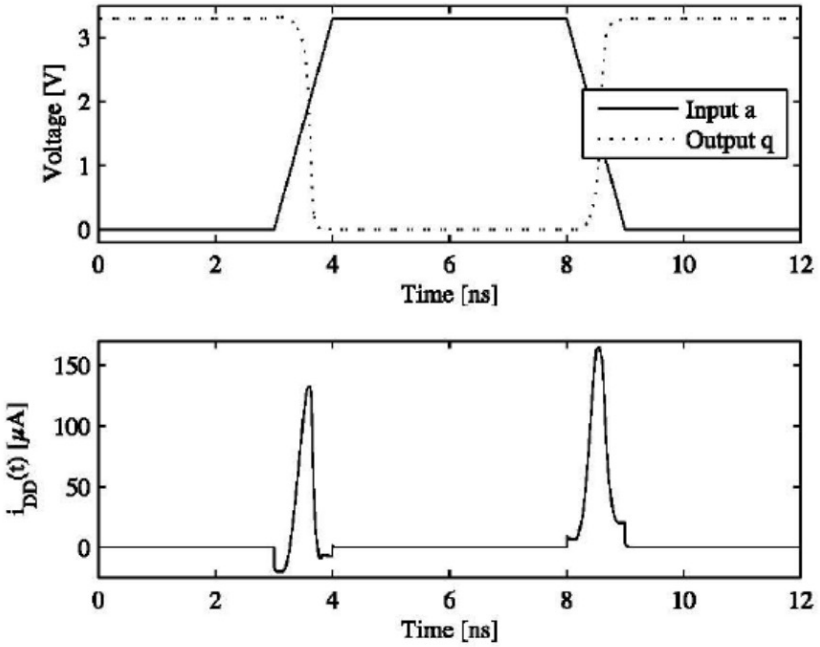
(b) Modular exponentiation (X^d mod N) calculation using left to right binary method



(c) Power dissipation model during modular exponentiation

::.. Side Channel Attack (9/11)

As power analysis utilizes the relationship between power consumption and the data being processed, dynamic power is the relevant one. As the static power is mostly constant, the variation in the total power is solely due to dynamic power and therefore the total power consumption can be directly used for an attack.



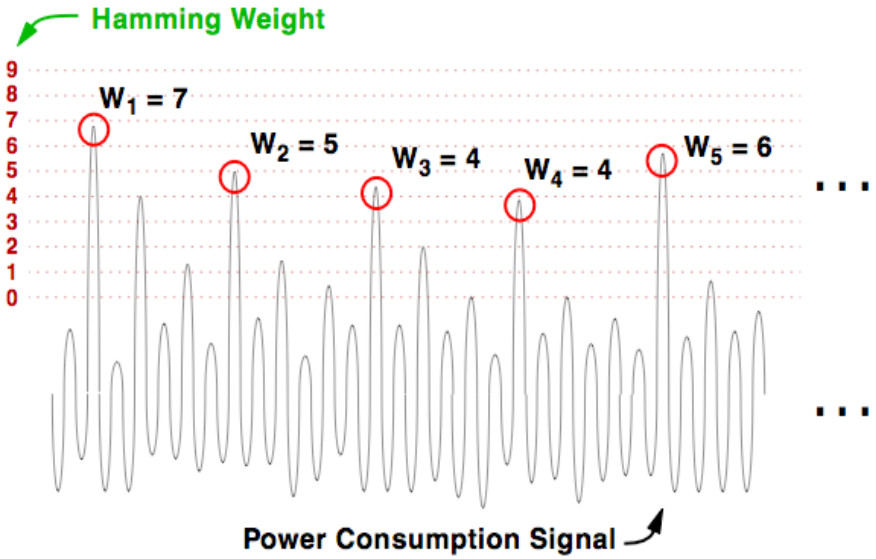
Dynamic power is consumed when switching occurs in transistors. That is if a CMOS cell changes from 0 to 1 or from 1 to 0, switching occurs in transistors and power is consumed.

A power model is used to deduce the power consumption of a circuit mathematically using the information we have about the circuit. Hamming distance model is a very simple.

::.. Side Channel Attack (10/11)

If the initial value on a piece of hardware, such as the bus, was v_0 and the value after the change is v_1, then the hamming distance can be simply found by counting the number of 0 to 1 and 1 to 0 transitions that happen.

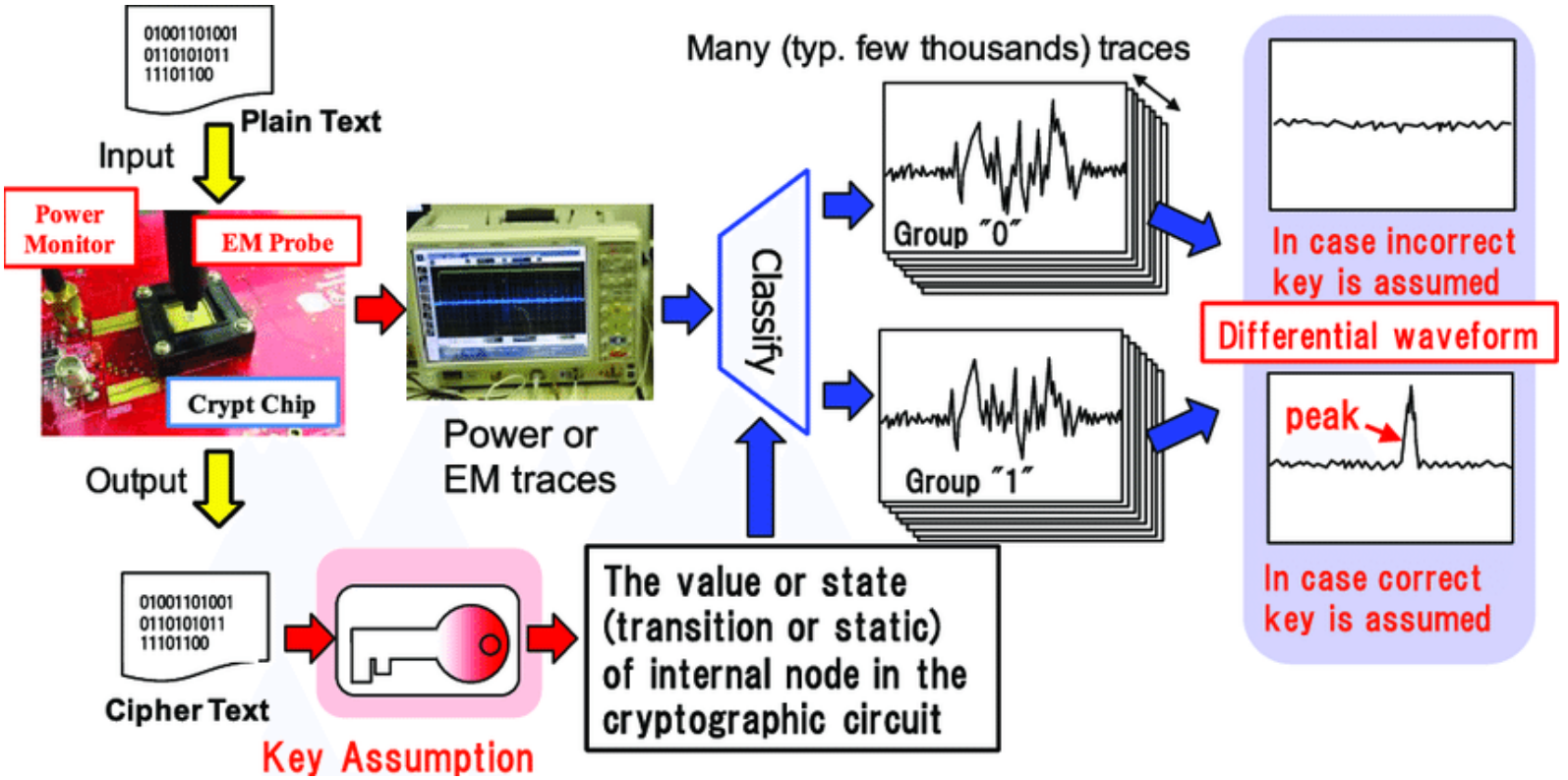
- If the data bus is four bits and if v_0 = 1010 and v_1 = 0011 only two bits have changed (first and the last), and therefore the hamming distance is equal to 2.



As the significant power consumption in the CMOS circuit occurs during transitions, we can infers the hamming distance between values by monitoring the power consumption.

::.. Side Channel Attack (11/11)

However, the power consumption also depends on the processed data, although the variations are smaller. Therefore, differential power analysis (DPA) attacks rely on statistical investigations of multiple traces in order to infer information about the processed data.



::.. Data Remanence Attack (1/3)

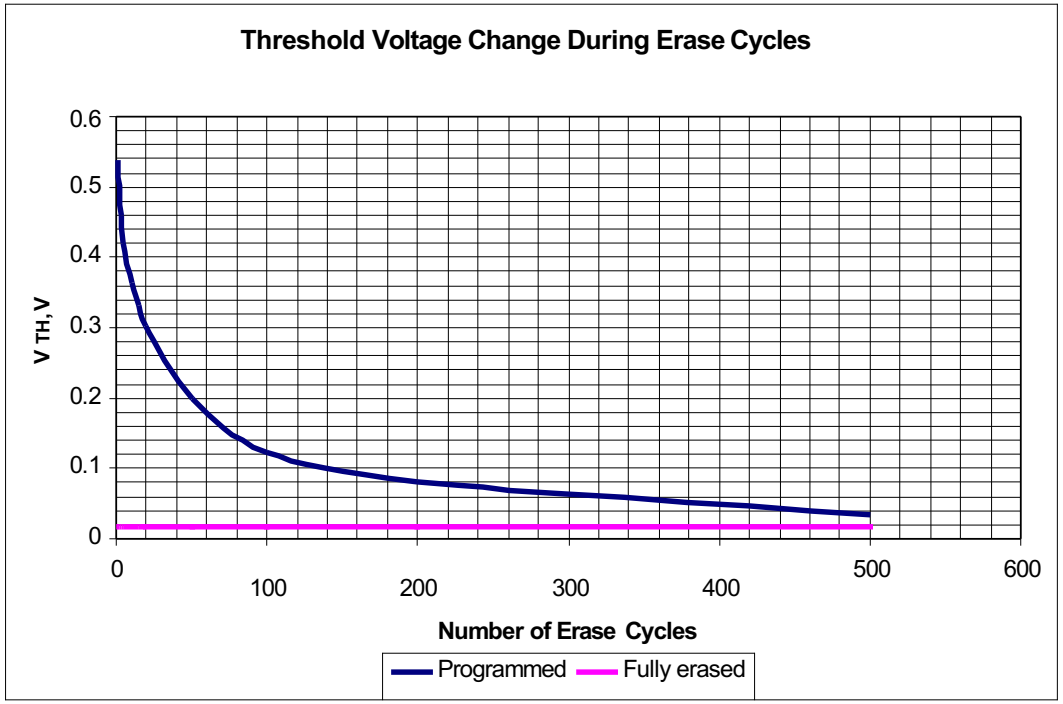
- Data remanence in SRAM
  - residual representation of data after erasure – first discovered in magnetic media then appeared to be the case for other memories
  - low temperature data remanence is dangerous to tamper resistant devices which store keys and secret data in a battery backed-up SRAM
  - 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

::.. Data Remanence Attack (2/3)

- 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

::.. Data Remanence Attack (3/3)

- 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



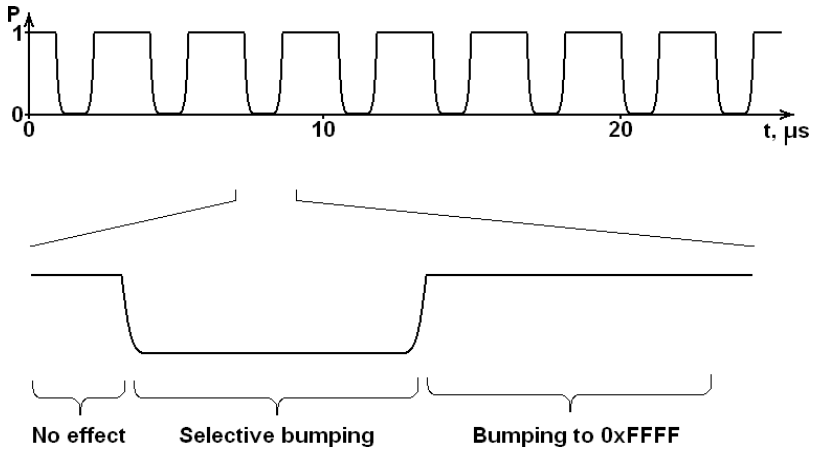
::.. Fault Injection Attack (1/2)

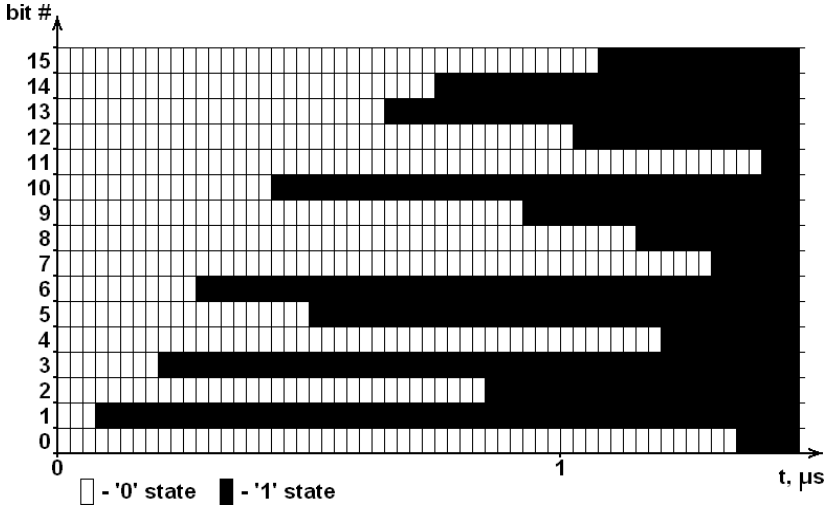
- Glitch attacks
  - clock glitches
  - power supply glitches
  - data corruption
- Security fuse verification in the Mask ROM bootloader of the Motorola MC68HC05B6 microcontroller
  - double frequency clock glitch causes incorrect instruction fetch
  - low-voltage power glitch results in corrupted EEPROM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

```
        LDA     #01h
        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:   … … …
```

::.. Fault Injection Attack (2/2)

- 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





::.. Brute Force Attack

- 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

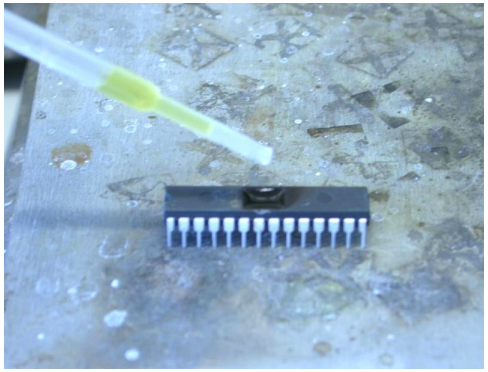
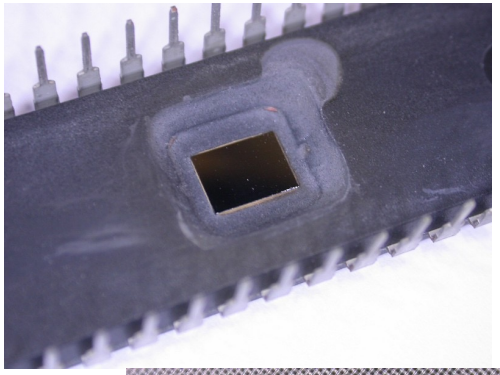
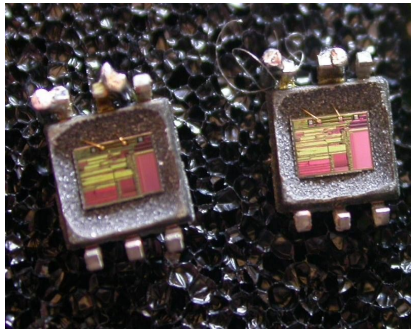
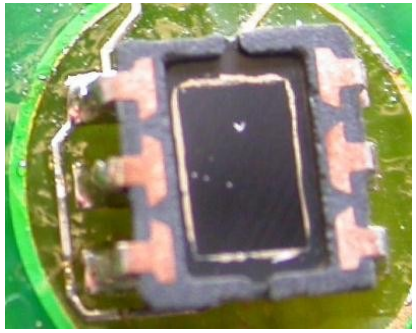
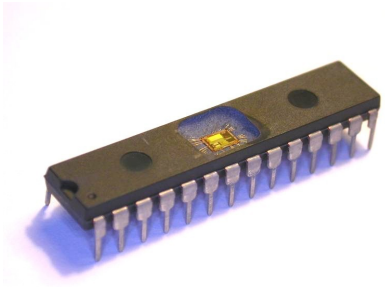
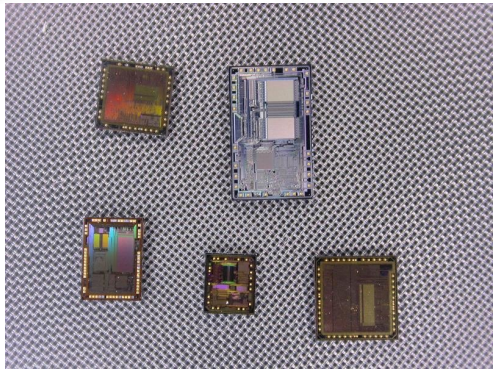
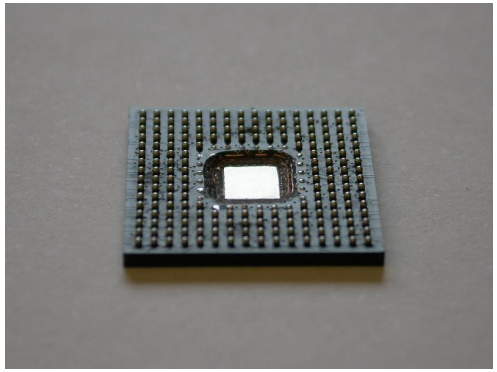
- Modern chips deter most brute force attacks
  - longer keys make searching infeasible
  - moving from 8-bit base to 32-bit base means longer search
  - CPLDs, FPGAs and ASICs became too complex to analyse
  - too large search field for finding hidden functionality

::.. Invasive Attacks (1/11)

- 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

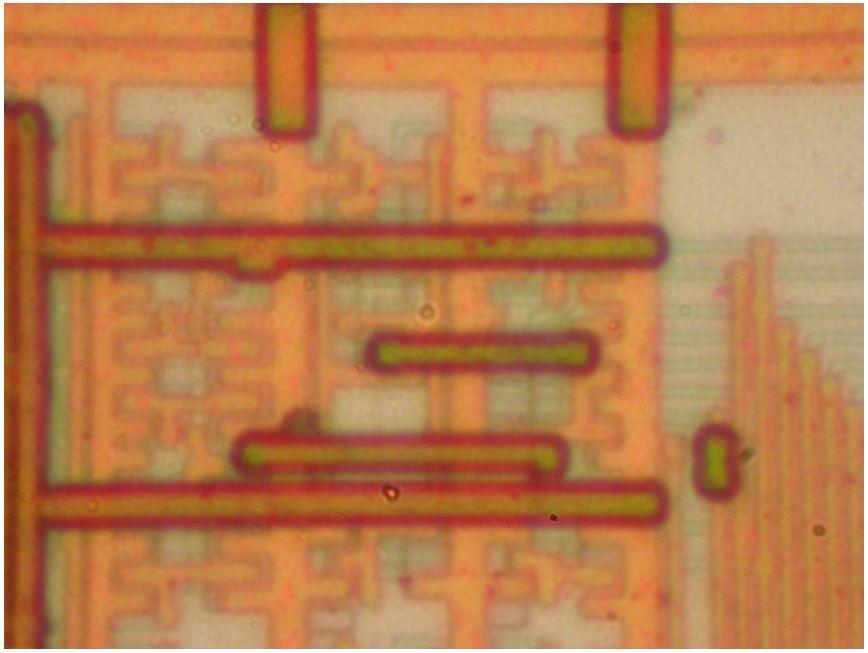
::.. Invasive Attacks (2/11)

- 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

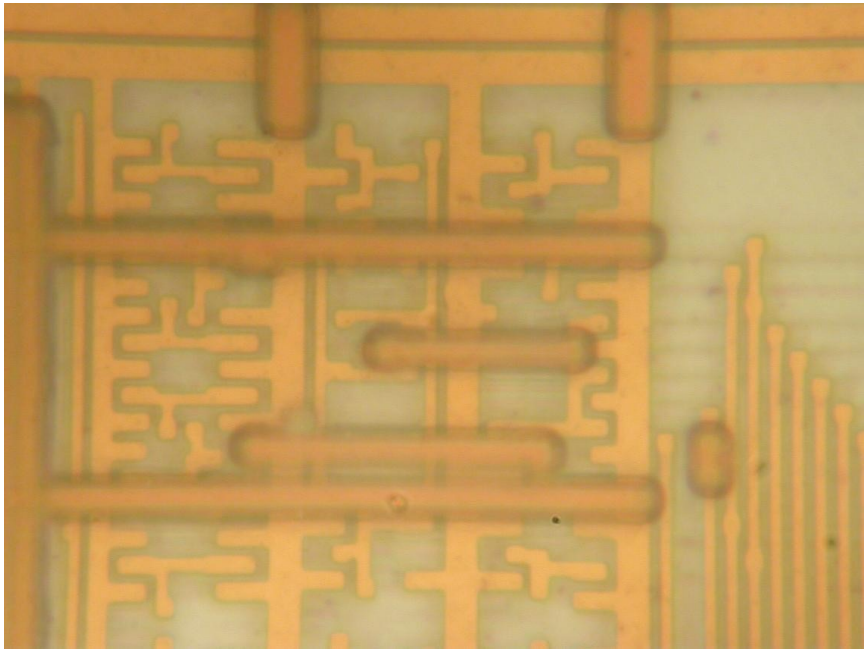








::.. Invasive Attacks (3/11)

- 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 ($n = 1.5$)



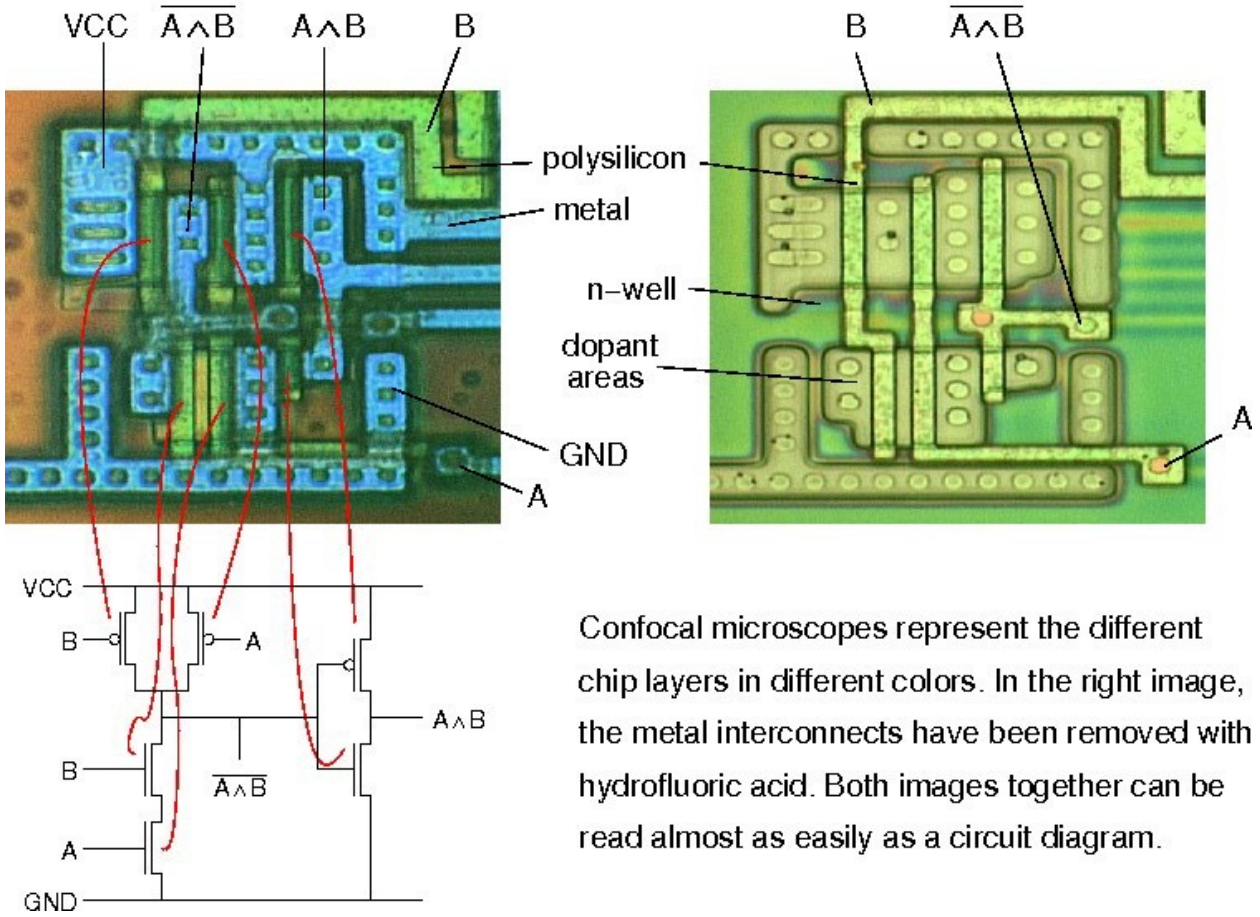
Bausch&Lomb MicroZoom, 50×2×, NA = 0.45



Leitz Ergolux AMC, 100×, NA = 0.9

::.. Invasive Attacks (4/11)

- 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



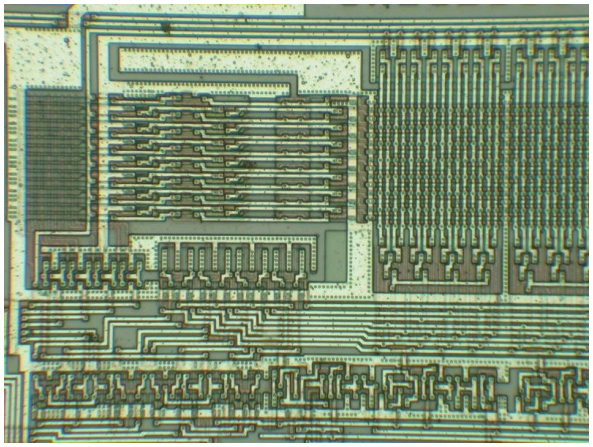
Confocal microscopes represent the different chip layers in different colors. In the right image, the metal interconnects have been removed with hydrofluoric acid. Both images together can be read almost as easily as a circuit diagram.

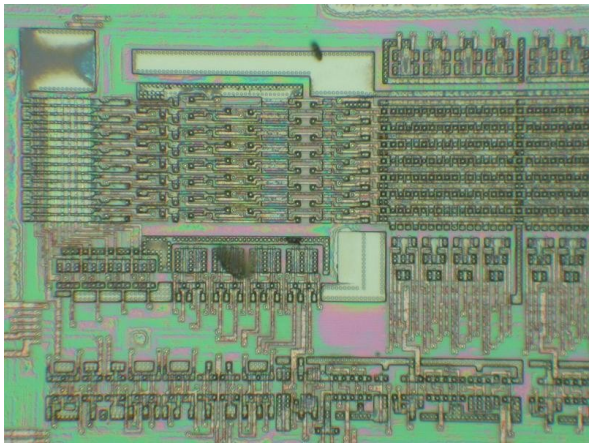
::.. Invasive Attacks (5/11)

- 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 (6/11)

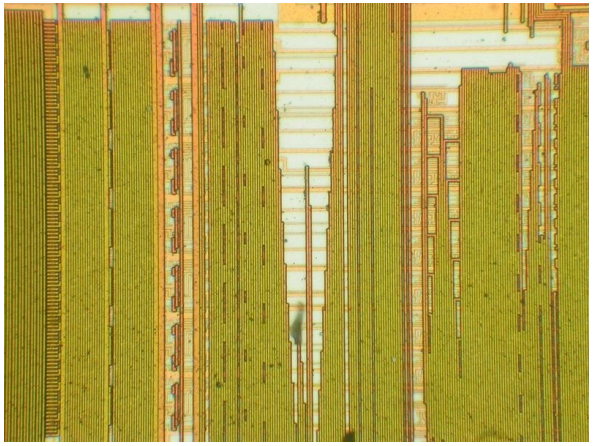
- Removing top metal layer using wet chemical etching
  - good uniformity over the surface, but works reliably only for chips fabricated with 0.8 µm or larger process (without polished layers)

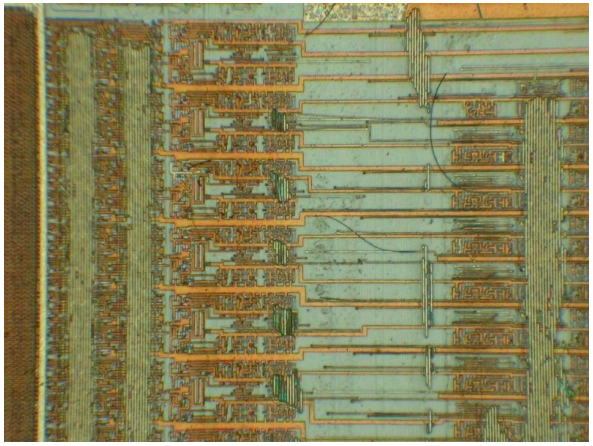




Motorola MC68HC705C9A microcontroller

1.0 µm



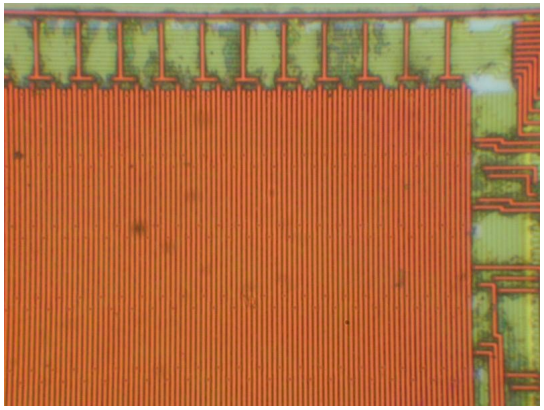


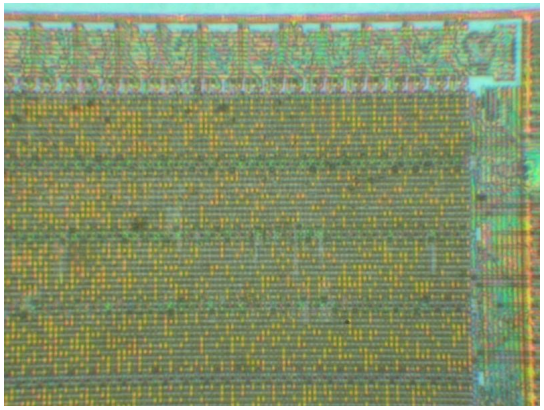
Microchip PIC16F76 microcontroller

0.5 µm

::.. Invasive Attacks (7/11)

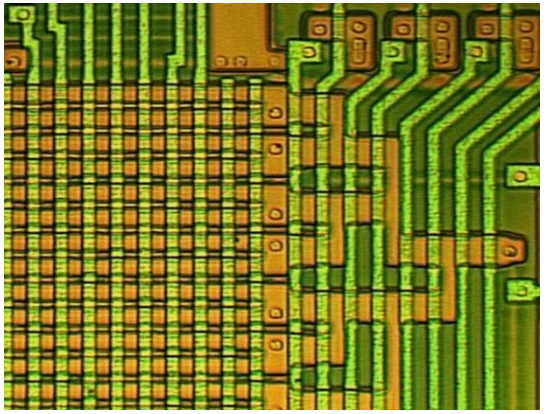
- Memory extraction from Mask ROMs
  - removing top metal layers for direct optical observation of data in NOR ROMs (bits programmed by presence of transistors)
  - not suitable for VTROM (ion implanted) used in smartcards – selective (dash) etchants are required to expose the ROM bits

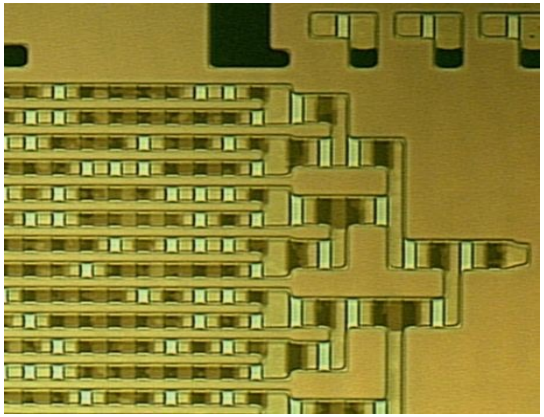




NEC µPD78F9116 microcontroller

0.35 µm





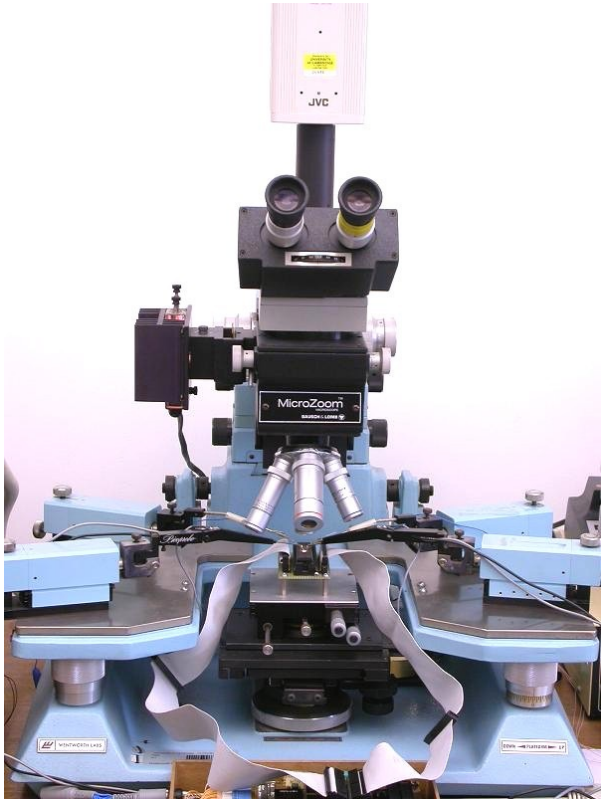
Motorola MC68HC05SC27 smartcard

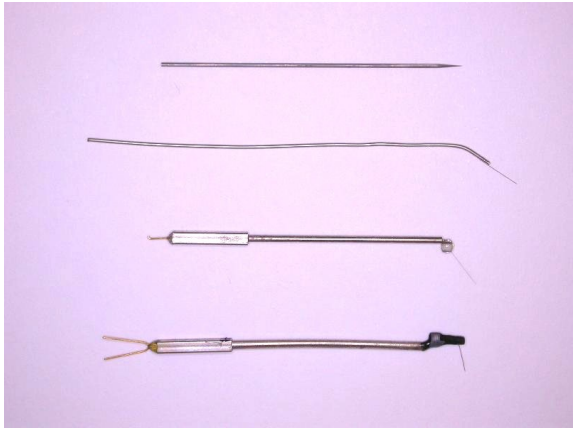
1.0 µm

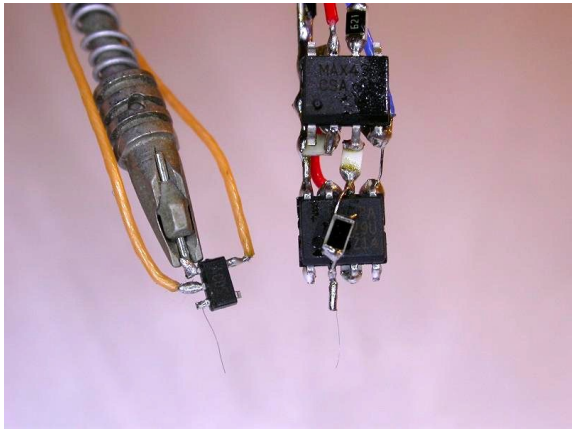
Picture courtesy of Dr Markus Kuhn

::.. Invasive Attacks (8/11)

- 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
  - limited use for 0.35µm and smaller chips

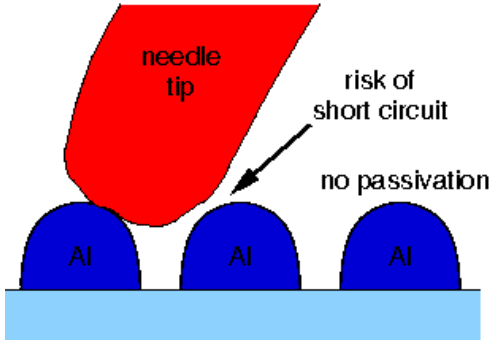


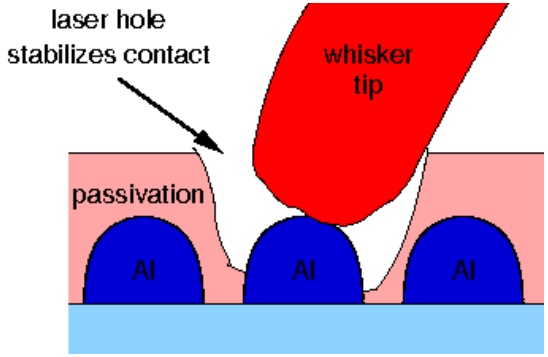




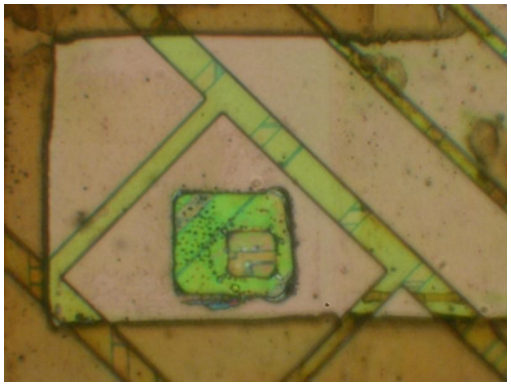
::.. Invasive Attacks (9/11)

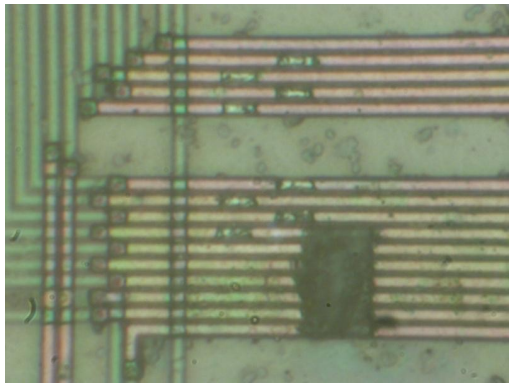
- Laser cutting systems
  - removing polymer layer from a chip surface
  - local removing of a passivation layer for microprobing attacks
  - cutting metal wires inside a chip
  - maximum can access the second metal layer





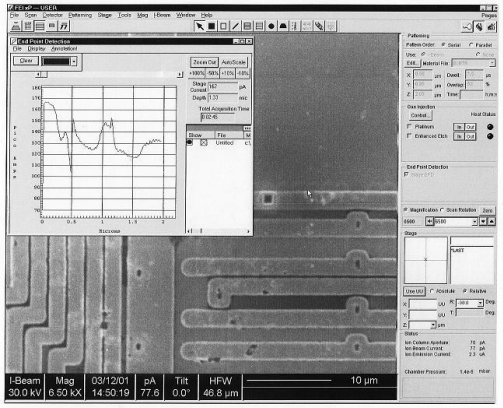
Picture courtesy of Dr Markus Kuhn

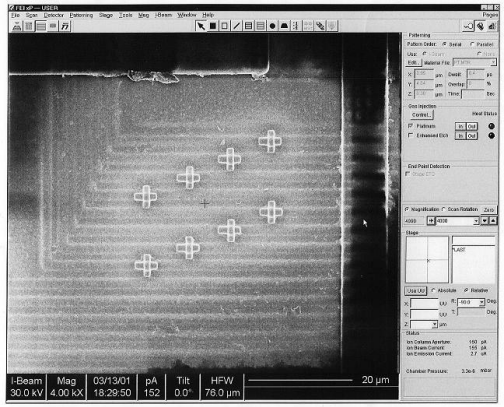




::.. Invasive Attacks (10/11)

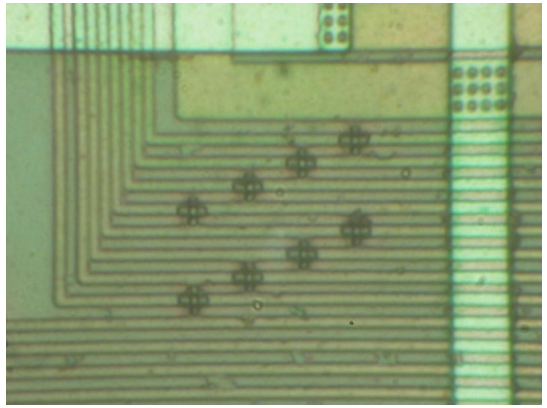
- Focused Ion Beam (FIB) workstation
  - chip-level surgery with 10 nm precision
  - etching with high aspect ratio
  - platinum and SiO_2 deposition

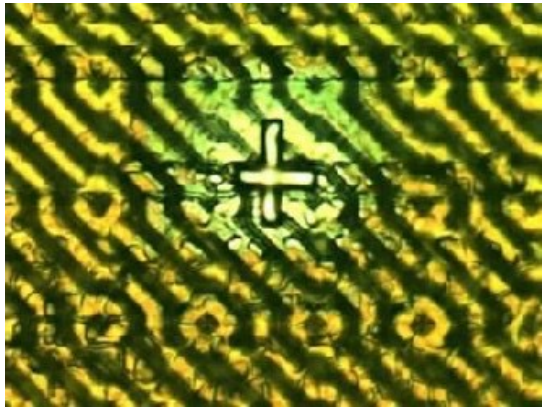




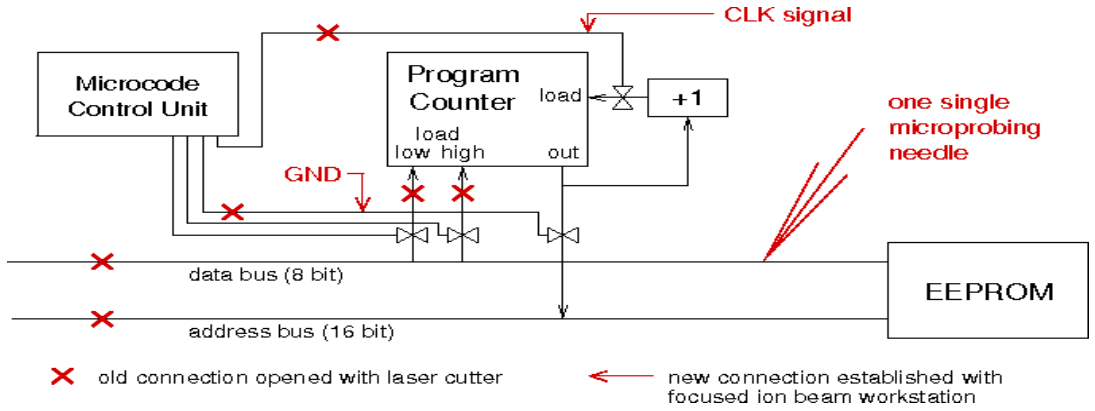
::.. Invasive Attacks (11/11)

- 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



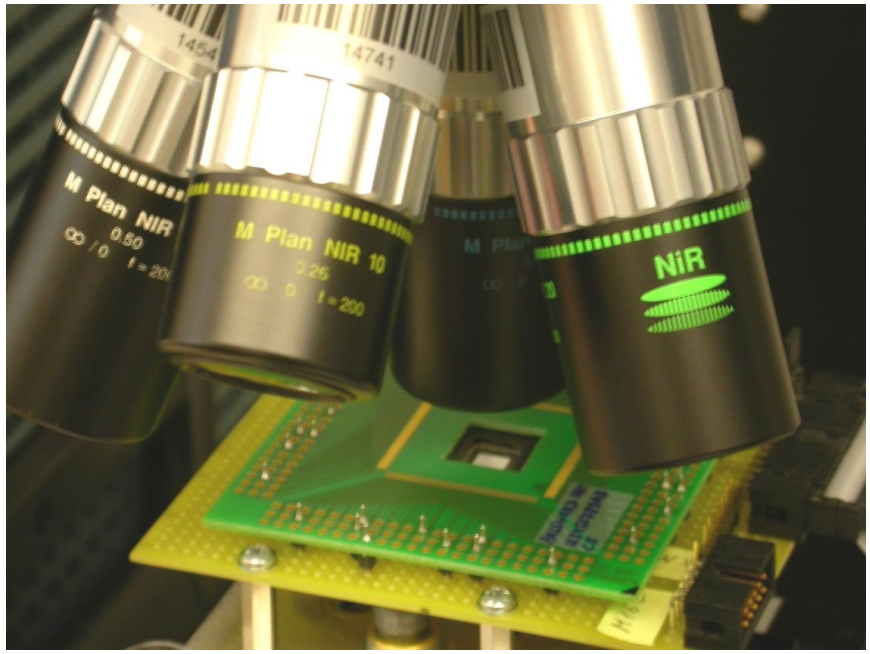
Picture courtesy of Dr Markus Kuhn

::.. Semi-Invasive Attacks (1/14)

- Fill 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: passive and active
  - imaging: optical and laser techniques
  - fault injection: UV attack, photon injection, local heating, masking
  - side-channel attacks: optical emission analysis, induced leakage

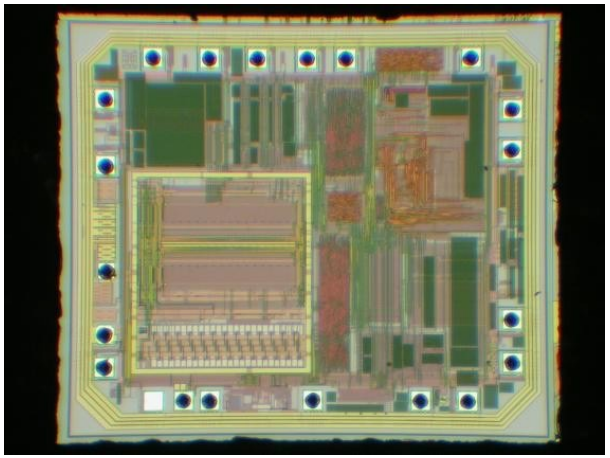
::.. Semi-Invasive Attacks (2/14)

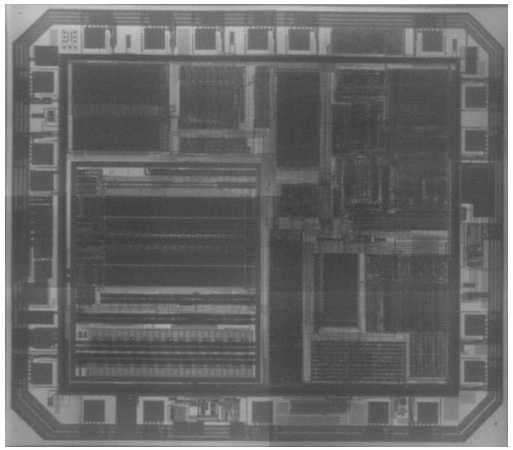
- Backside infrared imaging
  - microscopes with IR optics give better quality of image
  - IR-enhanced CCD cameras or special cameras must be used
  - resolution is limited to ~0.6μm by the wavelength of used light
  - view is not obstructed by multiple metal layers



::.. Semi-Invasive Attacks (3/14)

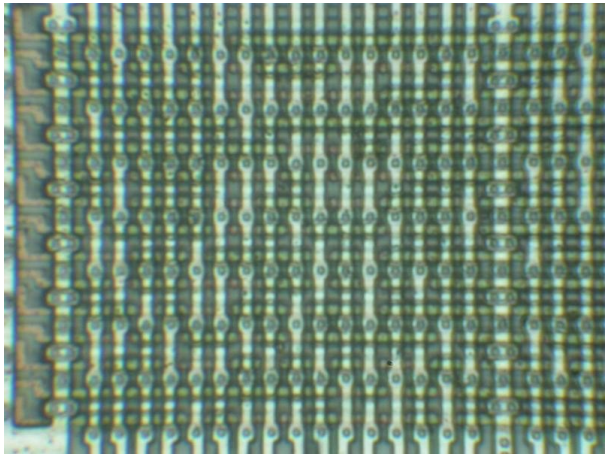
- Backside infrared imaging
  - Mask ROM extraction without chemical etching
- Main option for 0.35µm and smaller chips
  - multiple metal wires do not block the optical path

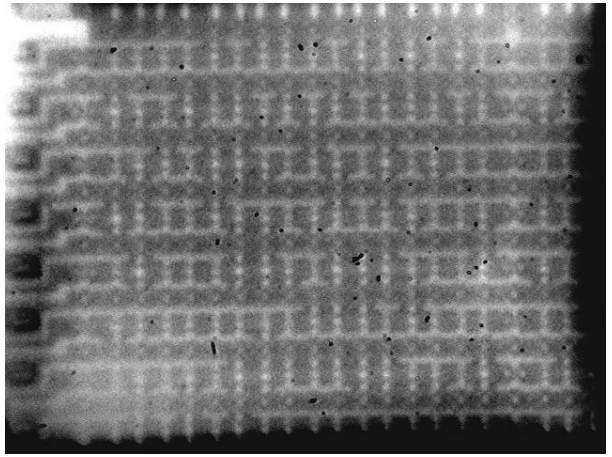




Texas Instruments MSP430F112 microcontroller

0.35 µm



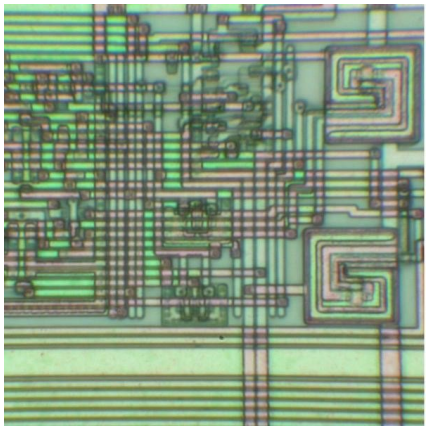


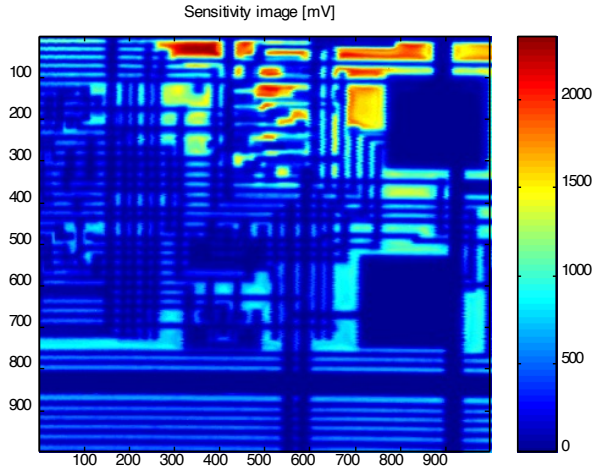
Motorola MC68HC705P6A microcontroller

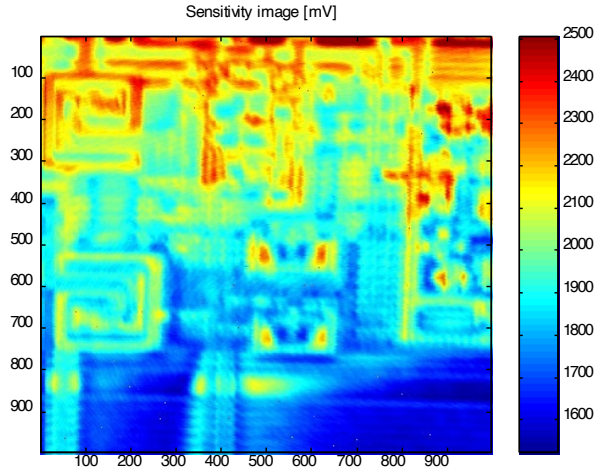
1.2 µm

::.. Semi-Invasive Attacks (4/14)

- 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 producing the image
  - used for localisation of active areas
  - also works from the rear side of a chip (using infrared lasers)



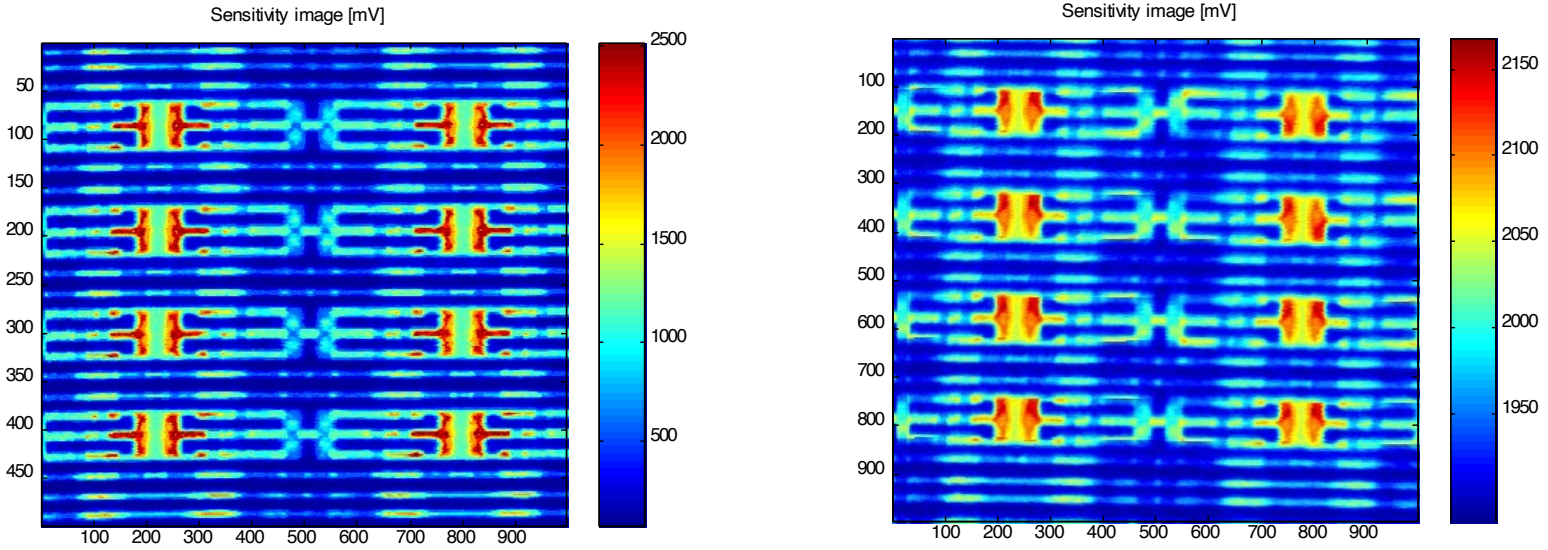




Microchip PIC16F84A microcontroller

::.. Semi-Invasive Attacks (5/14)

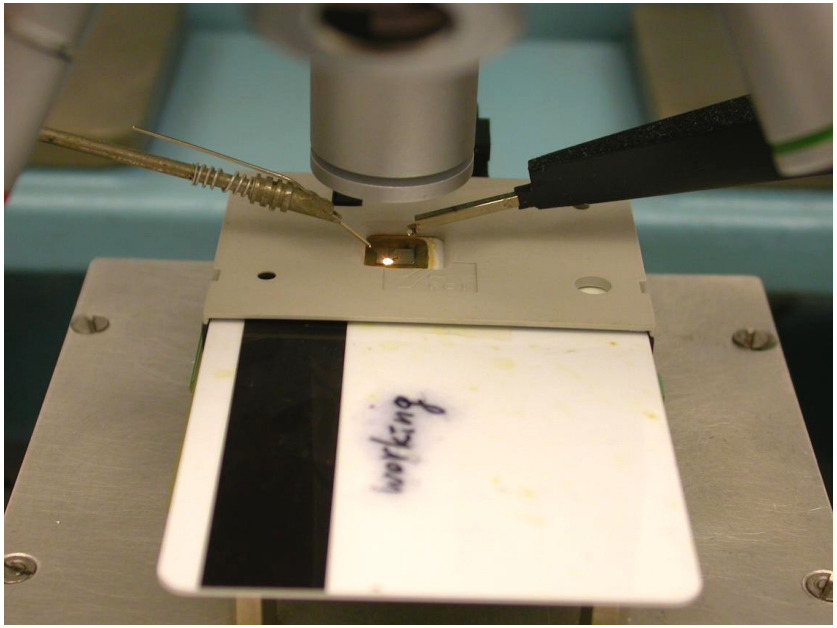
- Advanced imaging techniques – active photon probing (light-induced voltage alteration (LIVA) technique)
  - photon-induced photocurrent is dependable on the state of a transistor
  - reading logic state of CMOS transistors inside a powered-up chip
  - works from the rear side of a chip (using infrared lasers)
- Requires backside approach for 0.35µm and smaller chips
  - multiple metal wires do not block the optical path
  - resolution is limited to ~0.6µm (still enough for memory cells)

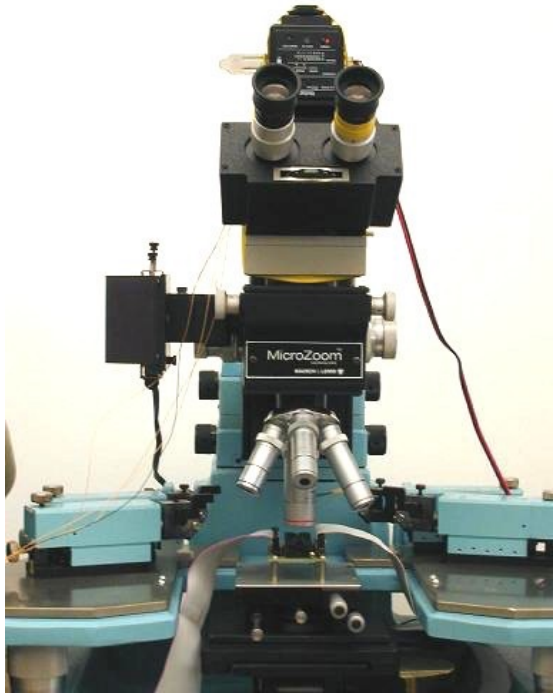


Microchip PIC16F84 microcontroller

::.. Semi-Invasive Attacks (6/14)

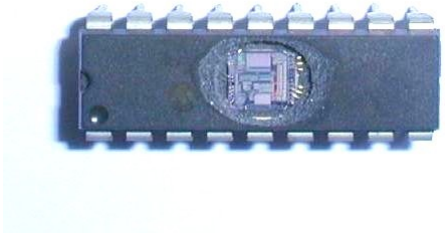
- Optical fault injection attacks
  - optical fault injection was observed with microprobing attacks in early 2001, introduced as a new method in 2002
  - lead to new powerful attack techniques and forced chip manufacturers to rethink their design and bring better protection
  - original setup involved optical microscope with a photoflash and Microchip PIC16F84 microcontroller programmed to monitor its SRAM



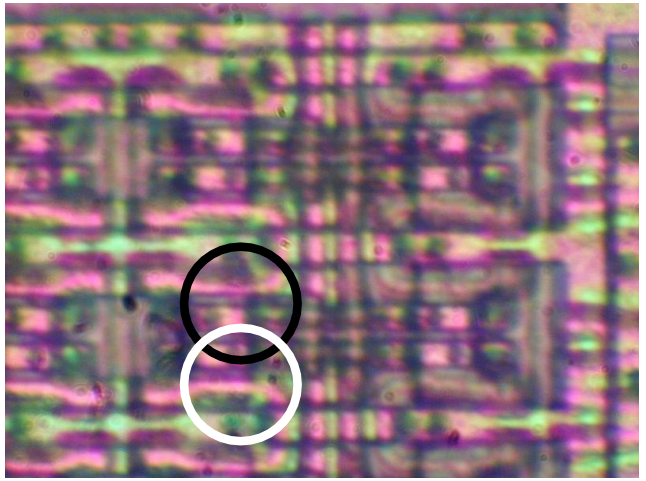


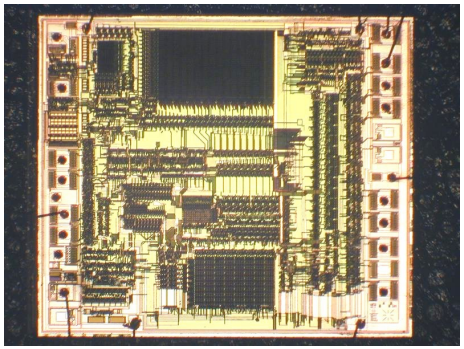
::.. Semi-Invasive Attacks (7/14)

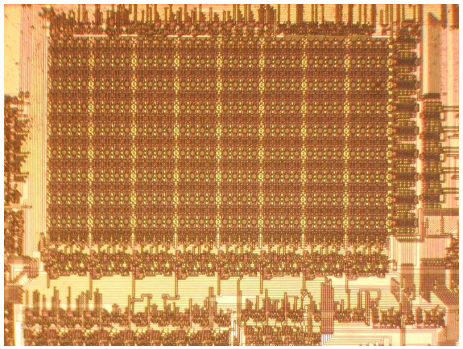
- Optical fault injection attacks
  - the chip was decapsulated and placed under a microscope
  - light from the photoflash was shaped with aluminium foil aperture
  - physical location of each memory address by modifying memory contents
  - the setup was later improved with various lasers and a better microscope
- Requires backside approach for 0.35µm and smaller chips
  - successfully tested on chips down to 130nm



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

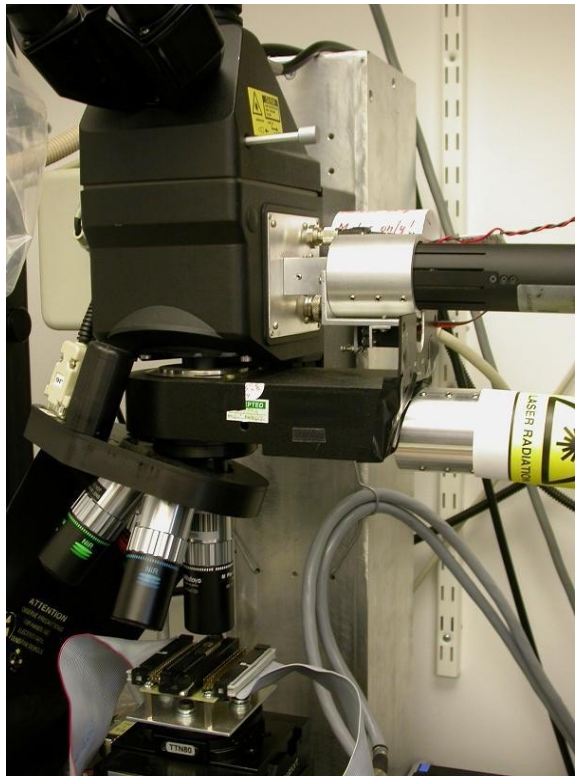


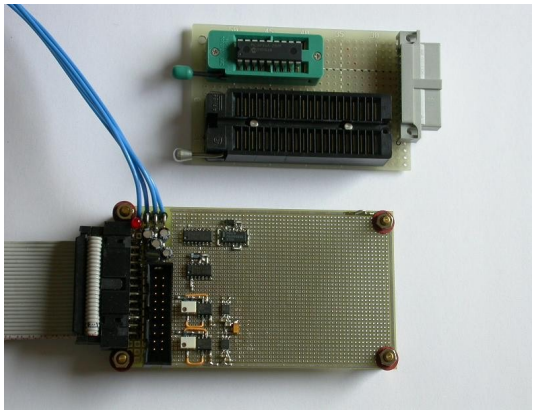


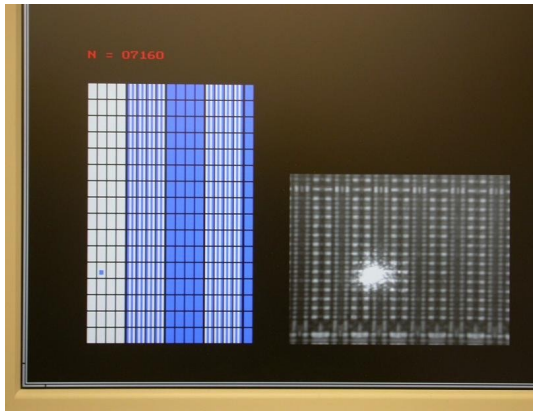


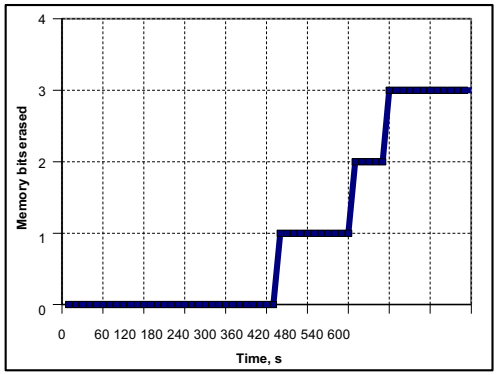
::.. Semi-Invasive Attacks (8/14)

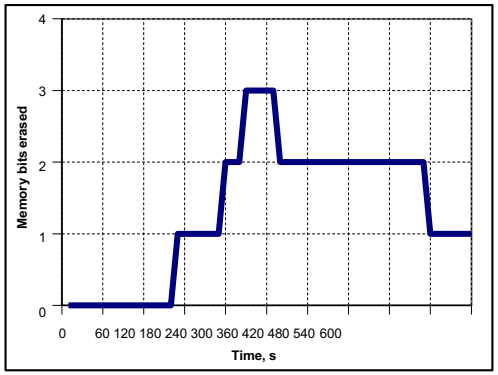
- Localised heating using cw lasers
  - test board with PIC16F628 and PC software for analysis
  - permanent change of a single memory cell on a 0.9µm chip
- Limited influence on modern chips (<0.5µm) – influence on adjacent cells







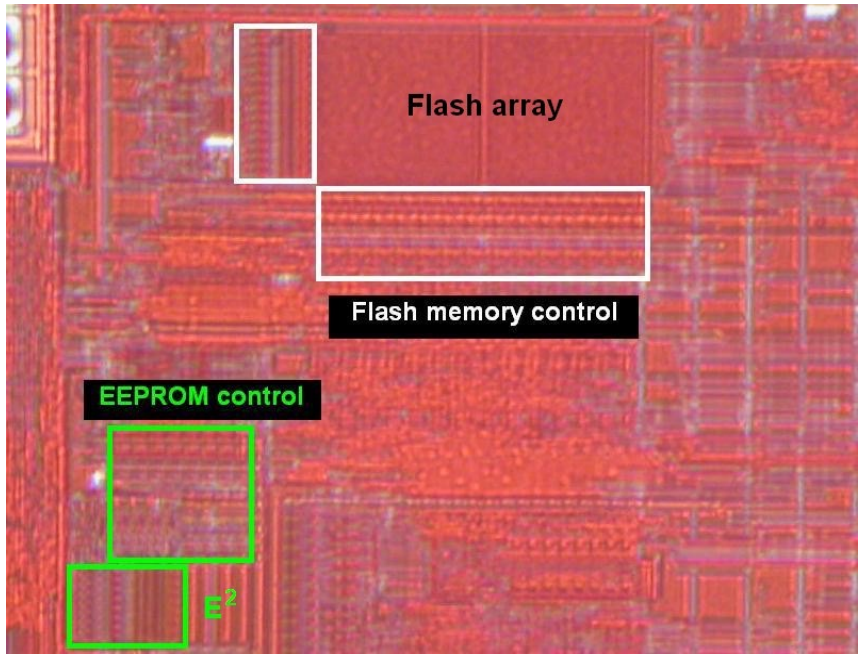


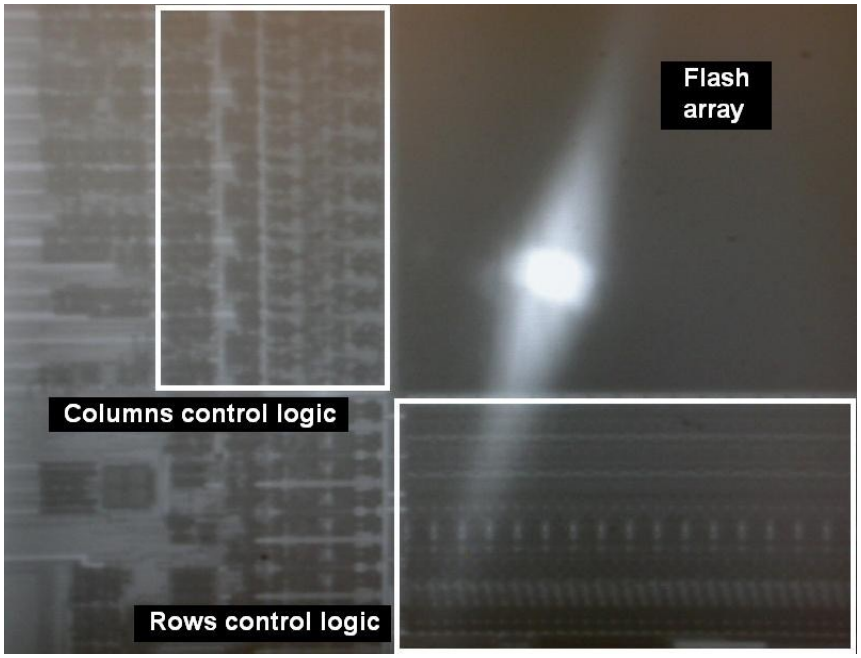


::.. Semi-Invasive Attacks (9/14)

- Memory masking attacks
  - temporarily disable write and erase operations in embedded memory (Flash/EEPROM) and write into volatile memory (SRAM)
  - use cw red lasers for front-side and infrared lasers for backside attacks

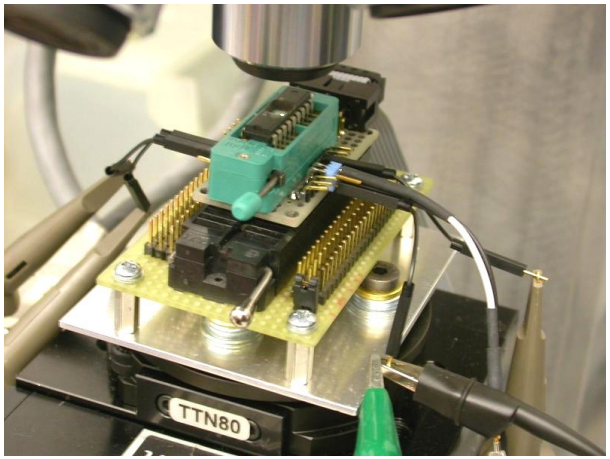
	Memory Write Operations					
Chip	***Flash Cells***	***Flash Lines***	***Flash Array***	***EEPROM Cell***	***EEPROM Lines***	***EEPROM Array***
PIC16F628A	1 – 2	1 – 2	Yes	1 – 2	1 – 2	Yes
PIC16F628A (backside)	12 – 45	1 – 2	Yes	8 – 22	1 – 2	Yes

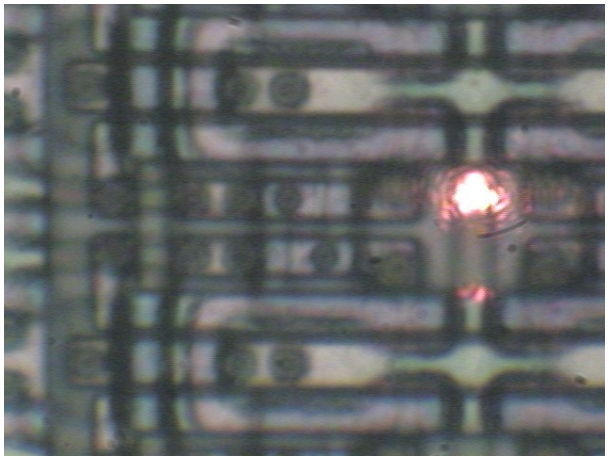


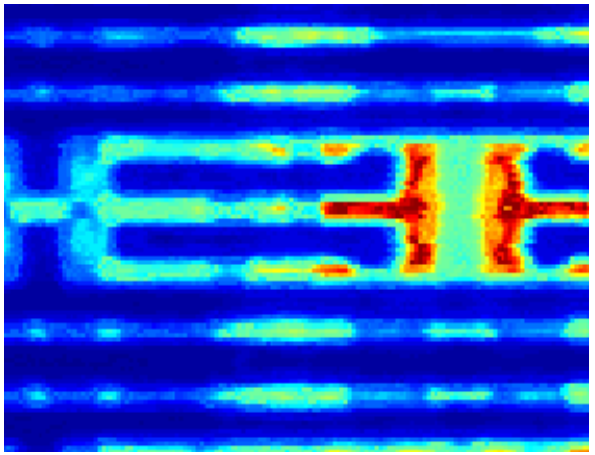


::.. Semi-Invasive Attacks (10/14)

- 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

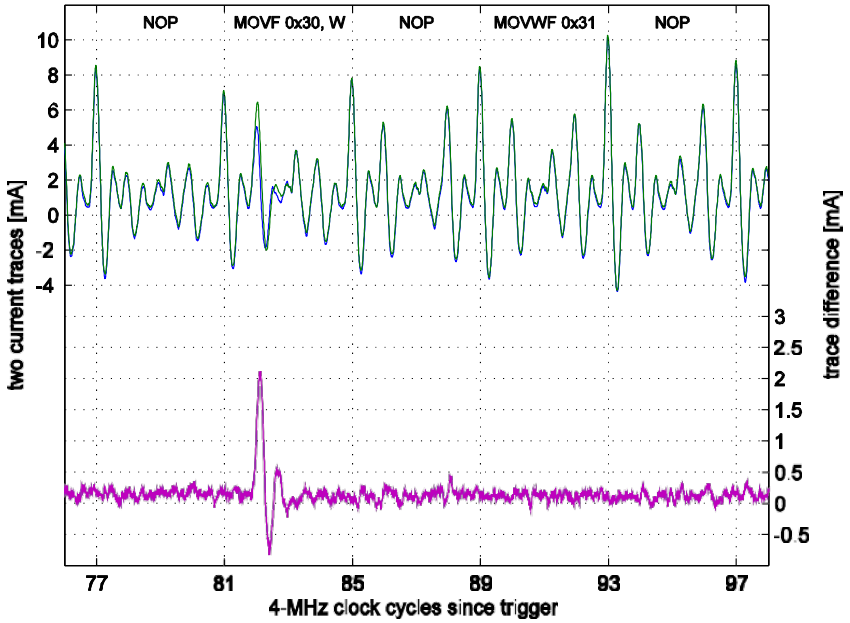


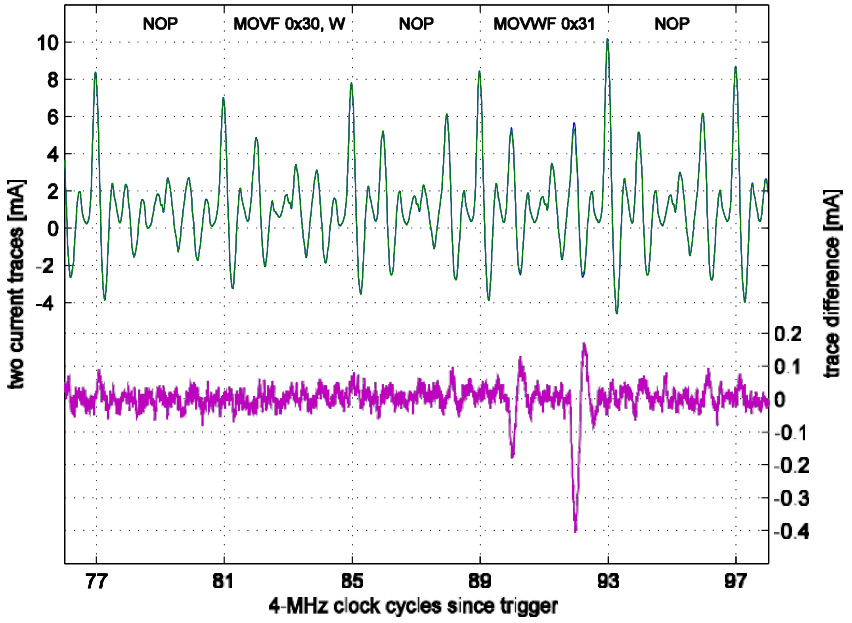




::.. Semi-Invasive Attacks (11/14)

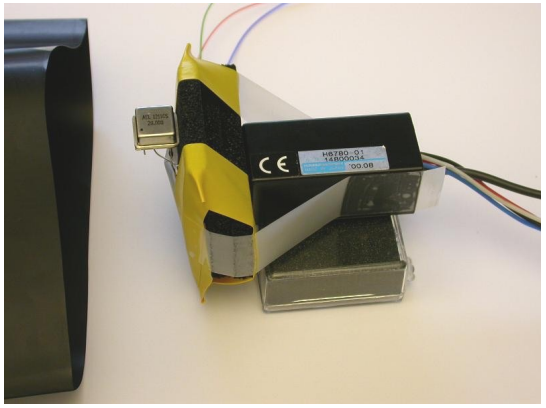
- Optically enhanced position-locked power analysis
  - results for memory read operations: non-destructive analysis of active memory locations (‘0’ and ‘1’)
  - results for memory write operations: non-destructive analysis of active memory locations (‘0→0’, ‘0→1’, ‘1→0’ and ‘1→1’)
- Only backside approach for 0.35µm and smaller chips
  - single-cell access is limited to 0.5µm laser spot

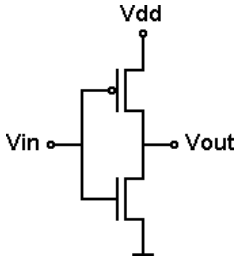


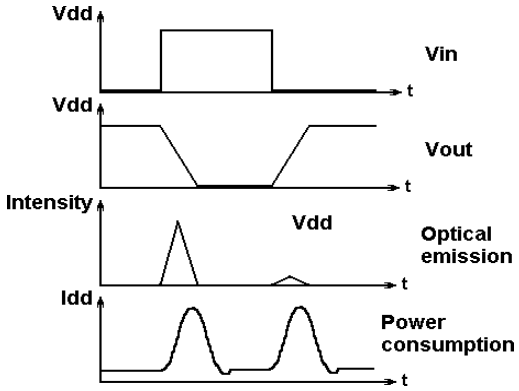


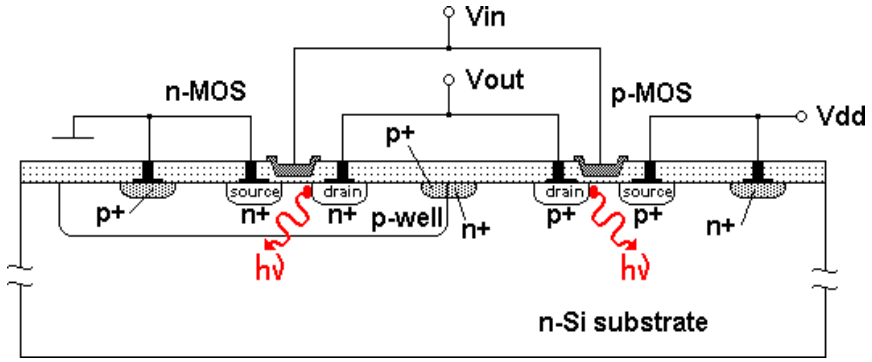
::.. Semi-Invasive Attacks (13/14)

- 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



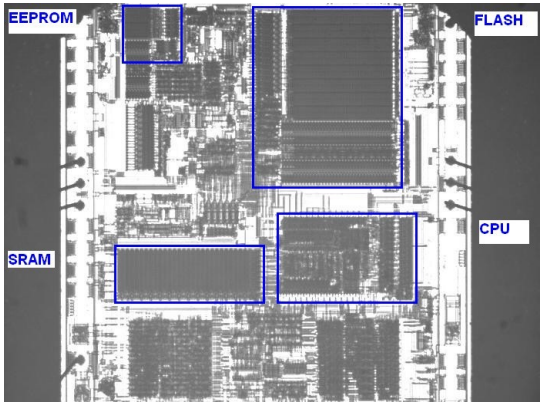


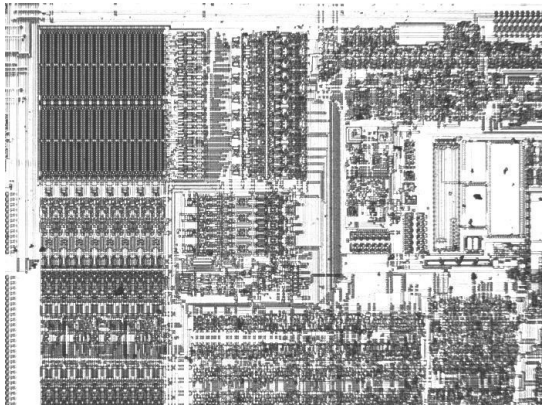


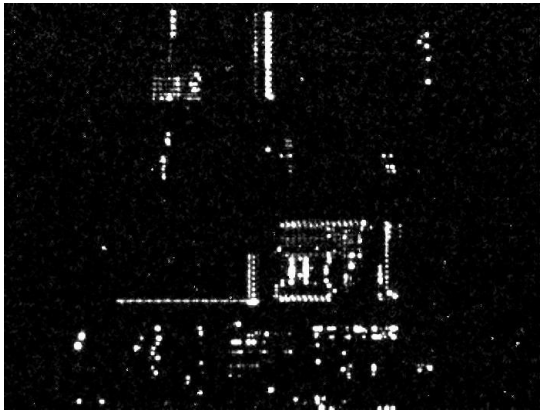


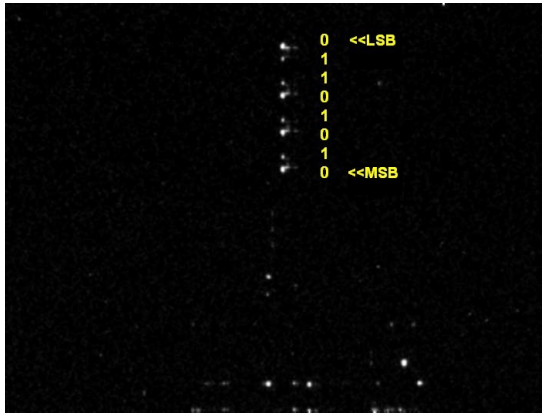
::.. Semi-Invasive Attacks (14/14)

- Optical emission analysis
  - Microchip PIC16F628 microcontroller with test code at 20 Mhz; PMT vs SPA and CCD camera images in just 10 minutes
- Only backside approach for 0.35µm and smaller chips
  - successfully tested on chips down to 130nm (higher Vcc, >1 hour)









::.. Sum-up

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

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

- Some semi-invasive attacks still effective on 130nm chips
- Recent publications showed that semi-invasive attacks still represent high security threat to modern chips

Protecting IoT Devices from Physical Attacks

::.. Tamper Resistance (1/8)

Tamper resistance mainly consists of a device's packaging being designed to make tampering difficult:

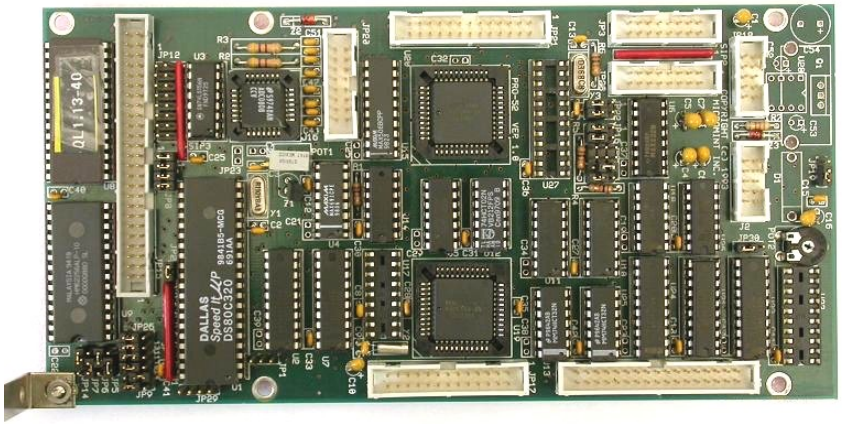
- Hardened steel enclosures;
- Locks;
- Encapsulation, potting;
- Security screws;
- Tight airflow channels.

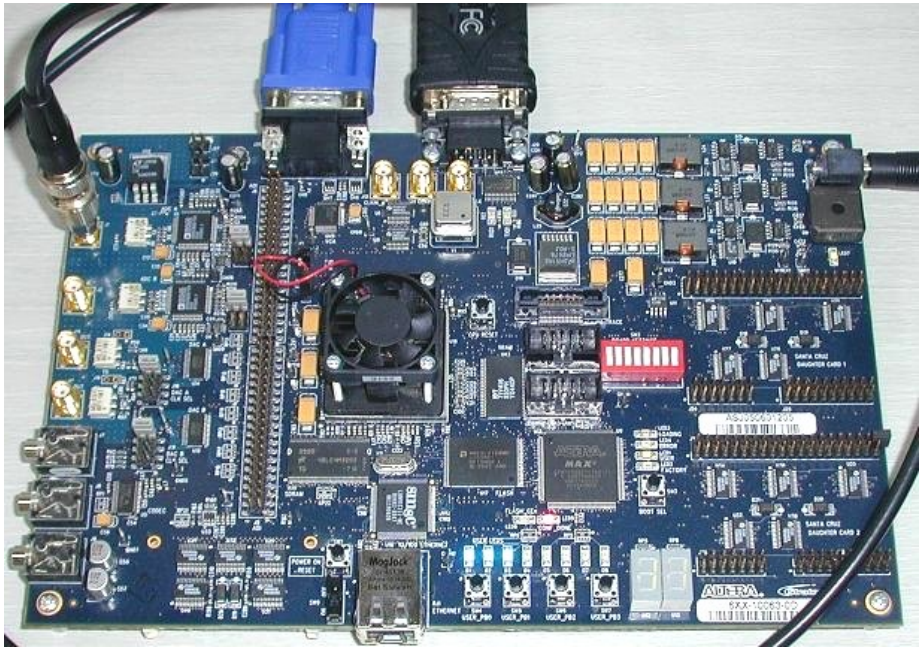
Most of these solutions are tamper evident, meaning that physical changes can be visually observed, so as to make obvious that the product has been tampered with.

Tamper evidence mechanisms are multiple, but most of them can be bypassed.

::.. Tamper Resistance (2/8)

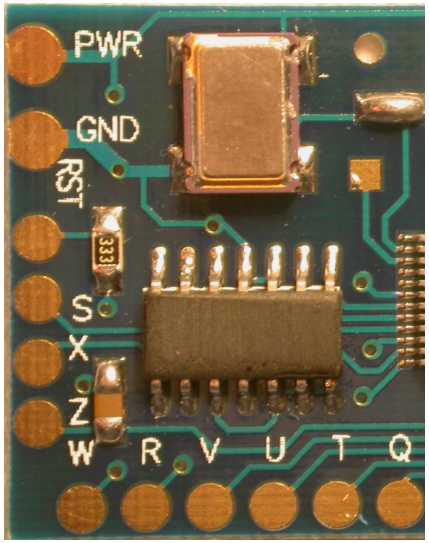
- Level ZERO (no special protection)
  - ✓ Microcontroller or FPGA with external ROM;
  - ✓ No special security features are used. All parts have free access and can be easily investigated;
  - ✓ Very low cost, attack time: minutes to hours.





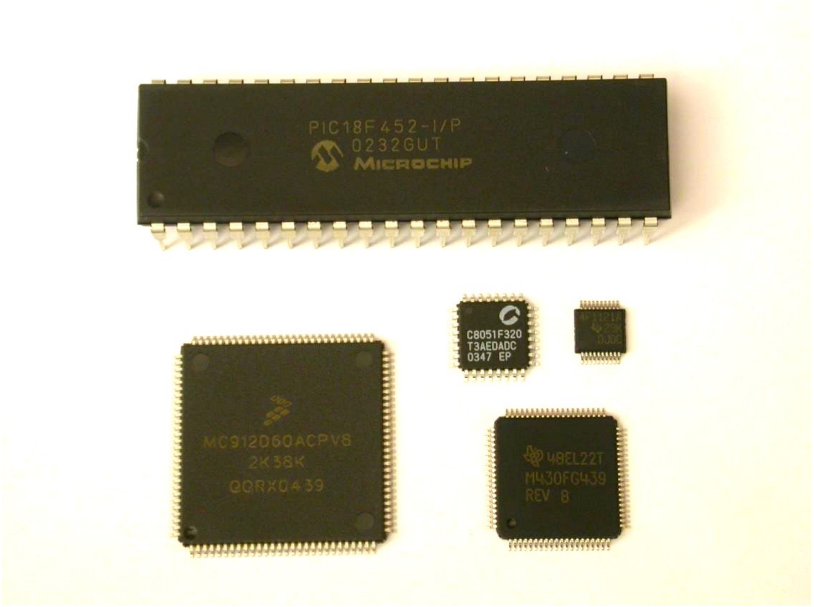
::.. Tamper Resistance (3/8)

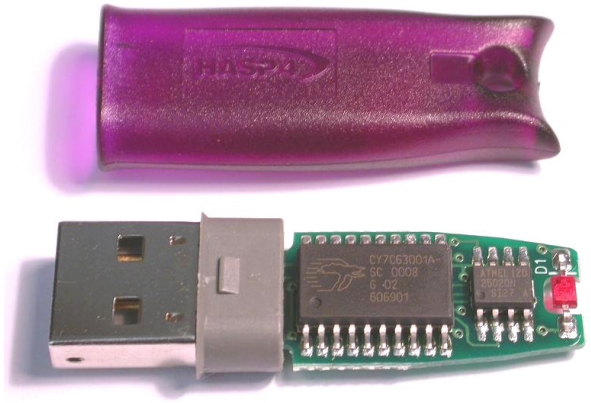
- Level LOW
  - ✓ Microcontrollers with proprietary access algorithm, remarked ICs;
  - ✓ Some security features are used but they can be relatively easy defeated with minimum tools required;
  - ✓ Low cost, attack time: hours to days.



::.. Tamper Resistance (4/8)

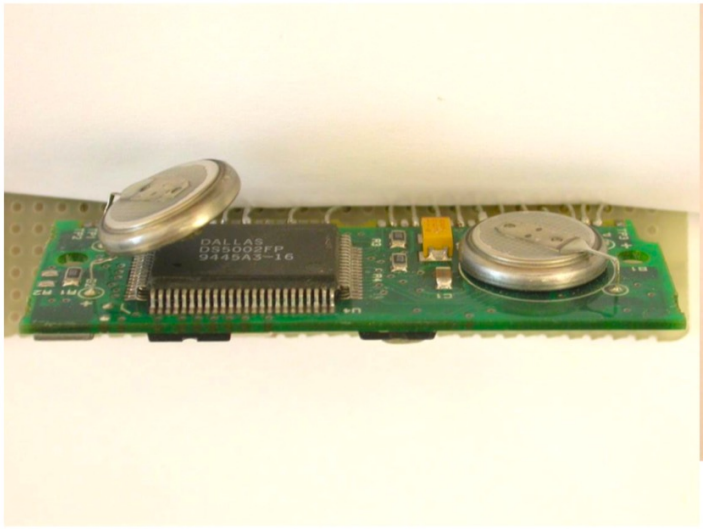
- Level MODL
  - ✓ Microcontrollers with security protection, low-cost hardware dongles;
  - ✓ Protection against many low-cost attacks;
  - ✓ Relatively inexpensive moderate cost, attack time: days to weeks.





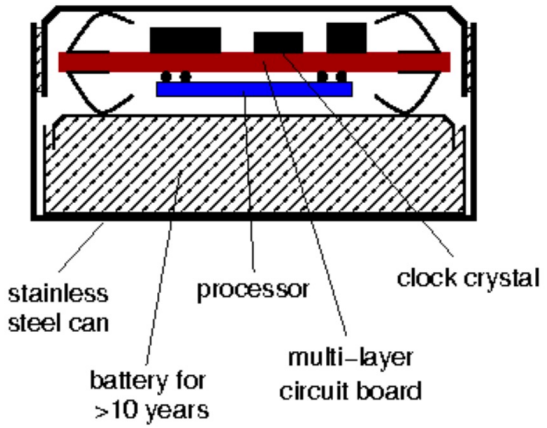
::.. Tamper Resistance (5/8)

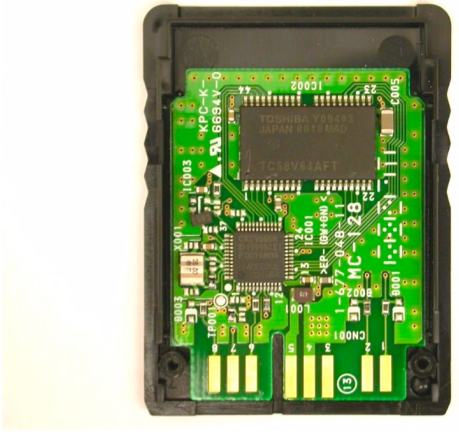
- Level MOD
  - ✓ Smartcards, high-security microcontrollers, ASICs, CPLDs, hardware dongles, i-Buttons, secure memory chips;
  - ✓ Special tools and equipment are required for successful attack as well as some special skills and knowledge;
  - ✓ High cost, attack time: weeks to months.



::.. Tamper Resistance (6/8)

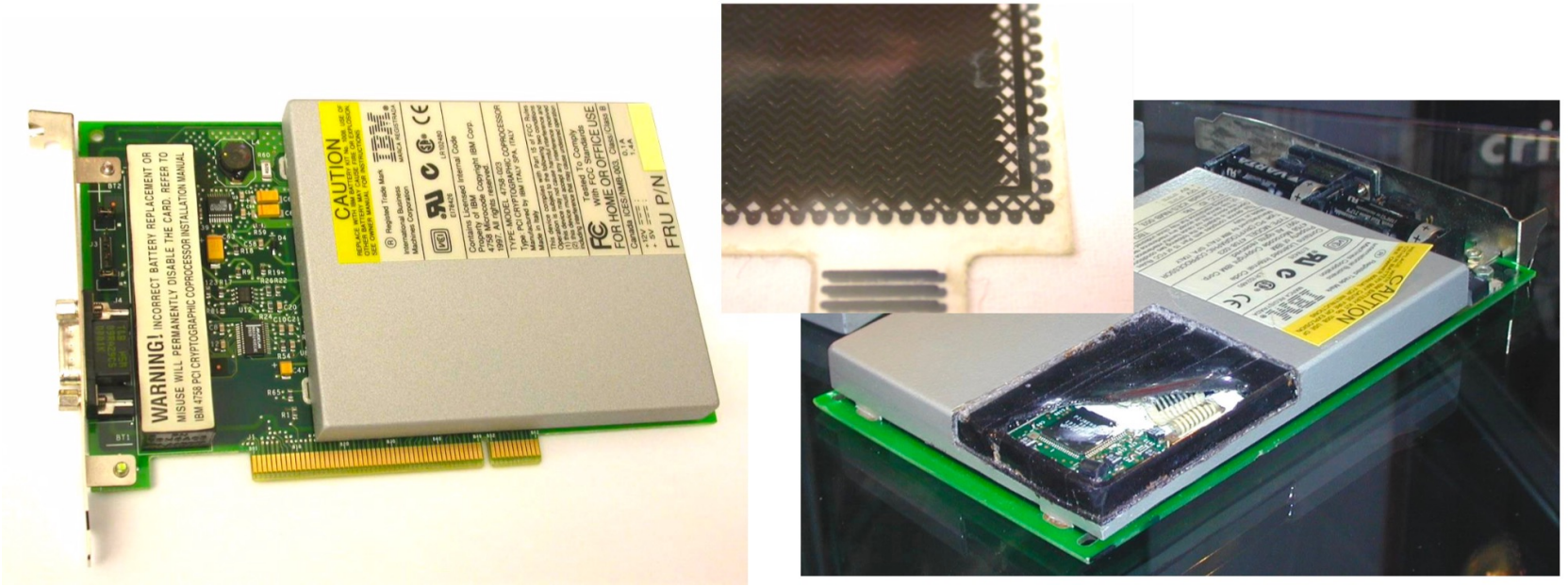
- Level MODH
  - ✓ Secure i-Buttons, secure FPGAs, high-end smartcards, ASICs, custom secure ICs
  - ✓ Special attention is paid to design of the security protection; equipment is available but is expensive to buy and operate
  - ✓ Very high cost, attack time: months to years





::.. Tamper Resistance (7/8)

- Level HIGH
  - ✓ Military and bank equipment;
  - ✓ Some research by a team of specialists is necessary to find a new attack, as all known attacks are defeated;
  - ✓ Extremely high cost, attack time: years



::.. Tamper Resistance (8/8)

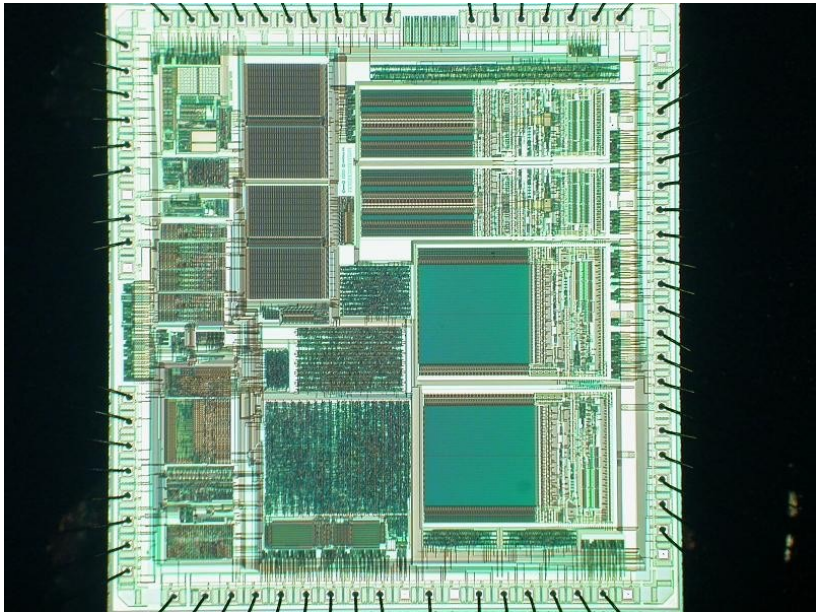
This division into levels from ZERO to HIGH is relative.

- 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
- The technological progress opens doors to less expensive attacks, thus reducing the protection level of some products

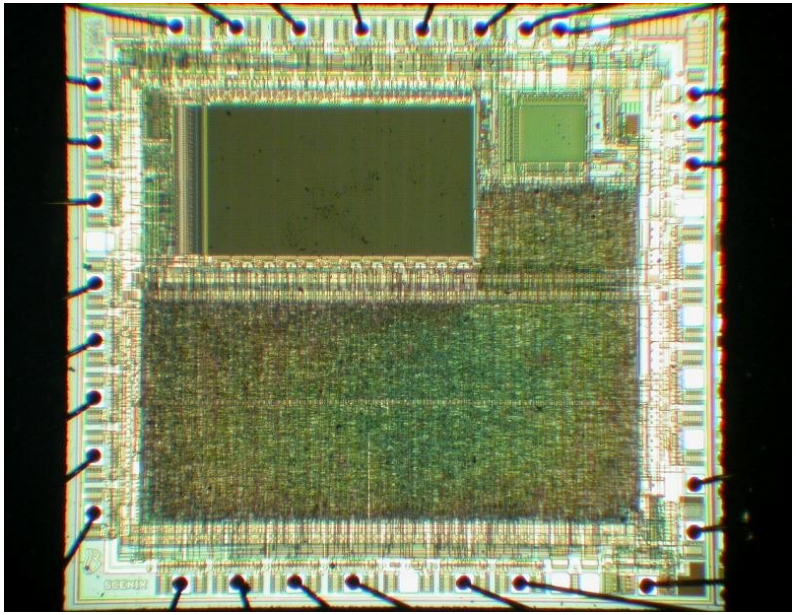
Proper security evaluation must be carried out to estimate whether products comply with all the requirements. It is crucial to run a design overview for any possible security flaws, and test products against known attacks.

::.. Tamper Protection (1/5)

- Old devices
  - 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
  - moving away from building blocks which are easily identifiable and have easily traceable data paths



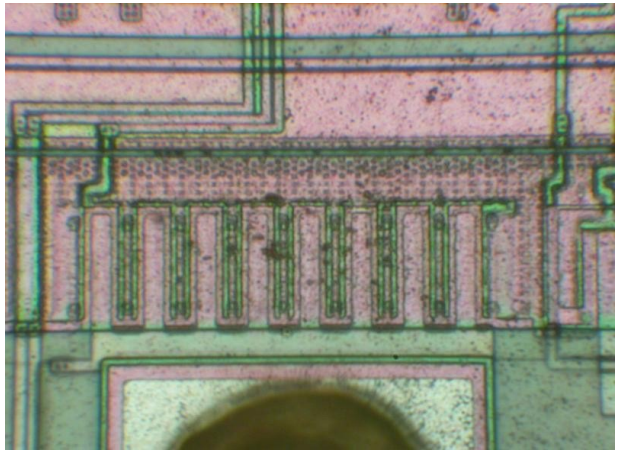
Motorola MC68HC908AZ60A microcontroller



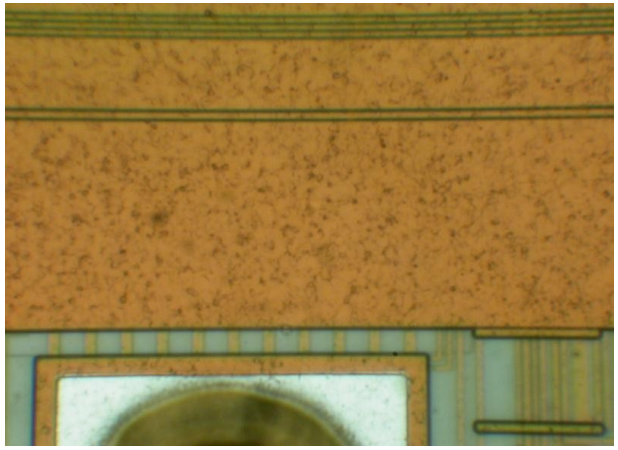
Scenix SX28 microcontroller

::.. Tamper Protection (2/5)

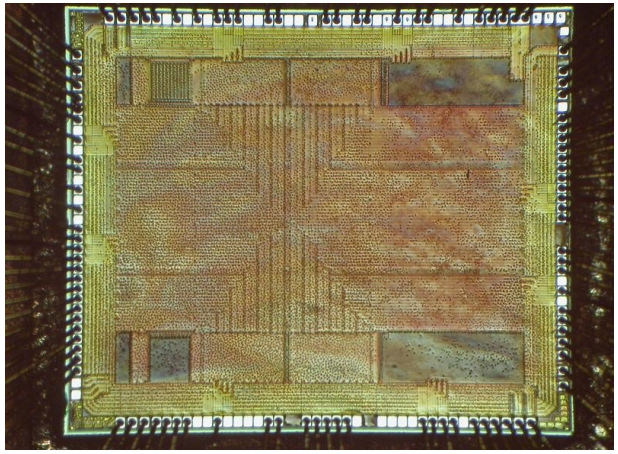
- Help came from chip fabrication technology
  - planarisation as a part of modern chip fabrication process (0.5 µm or smaller feature size)
  - glue logic design makes reverse engineering much harder
  - multiple metal layers block any direct access
  - small size of transistors makes attacks less feasible
  - chips operate at higher frequency and consume less power
  - smaller and BGA packages scare off many attackers



0.9µm microcontroller



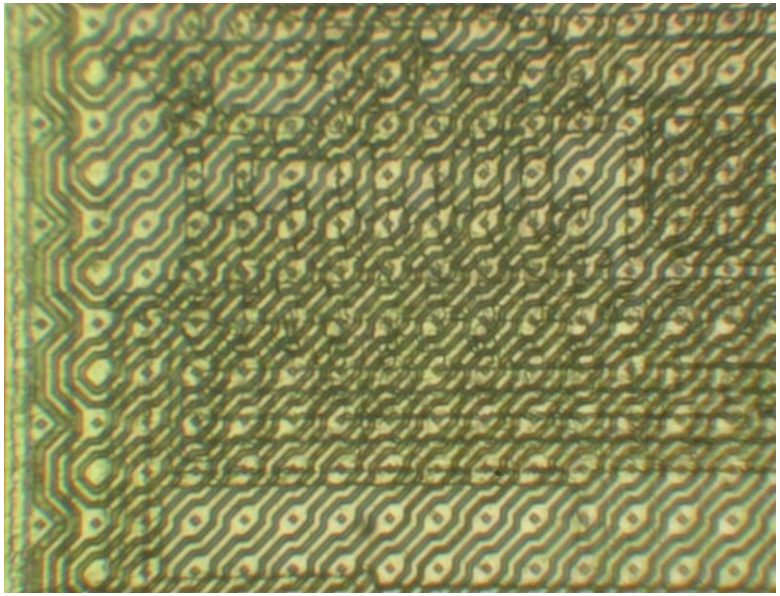
0.5µm microcontroller



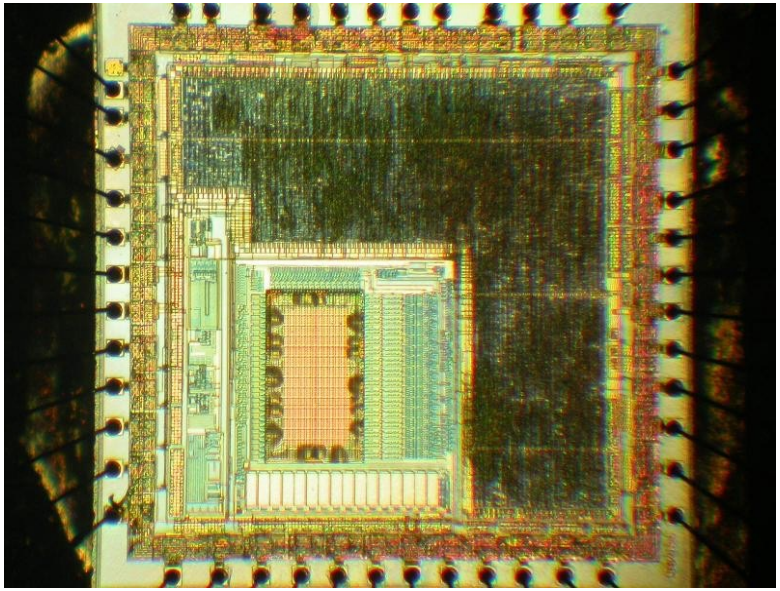
0.13µm FPGA

::.. Tamper Protection (3/5)

- Additional protections
  - top metal layers with sensors
  - voltage, frequency and temperature sensors
  - memory access protection, crypto-coprocessors
  - internal clocks, power supply pumps
  - asynchronous logic design, symmetric design, dual-rail logic
  - ASICs, secure FPGAs and custom-designed ICs
  - software countermeasures



STMicroelectronics ST16 smartcard



Fujitsu secure microcontroller

::.. Tamper Protection (4/5)

- Security advertising without proof
  - no means of comparing security, lack of independent analysis
  - no guarantee and no responsibility from chip manufacturers
  - wide use of magic words: *protection, encryption, authentication, unique, highly secure, strong defence, cannot be, unbreakable, impossible, uncompromising, buried under x metal layers*
- Constant economics pressure on cost reduction
  - less investment, hence, cheaper solutions and outsourcing
  - security via obscurity approach
- Quicker turnaround
  - less testing, hence, more bugs
- What about back-doors?
  - access to the on-chip data for factory testing purposes
  - how reliably was this feature disabled?
  - how difficult is to attack the access port?
  - are there any trojans deliberately inserted by subcontractors?

::.. Tamper Protection (5/5)

- Microchip PIC microcontroller: security fuse bug
  - security fuse can be reset without erasing the code/data memory
    - solution: fixed in newer devices
- Hitachi smartcard: information leakage on a products CD
  - full datasheet on a smartcard was placed by mistake on the CD
- Actel secure FPGA: programming software bug
  - devices were always programmed with a 00..00 passkey
    - solution: software update
- Xilinx secure CPLD: programming software bug
  - security fuse incorrectly programmed resulting in no protection
    - solution: software update
- Dallas SHA-1 secure memory: factory initialisation bug
  - some security features were not activated resulting in no protection
    - solution: recall of the batch
- Other possible ways of security failures
  - insiders, datasheets of similar products, development tools, patents
    - solution: test real devices and control the output