Semi-Invasive Extension to Physical Attacks

Dr Sergei Skorobogatov

Computer Security Group

Email: sps32@cam.ac.uk URL: www.cl.cam.ac.uk/~sps32/

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Physical attacks

Attacks that involve direct manipulation with devices (signal tampering or injection, modification, reverse engineering…)

Area of interest: Hardware security of semiconductor chips (maintaining confidentiality and integrity of information)

- Microcontrollers
- ASICs
- Custom ICs
- Smartcards
- Security modules

Reasons for learning attack technologies

- Understanding how and why the attacks work
- Estimating capabilities of the attackers
- Locating the most sensitive points in the design
- Developing much better protected hardware

Attack methods

Non-invasive attacks: side-channel, brute force, glitching…

- Observe or manipulate with the device without physical harm to it
- Require only moderately sophisticated equipment and knowledge to implement
- Normally do not leave evidence of the attack
- Many are reversible

Invasive attacks: reverse engineering, microprobing, modification…

- Almost unlimited capabilities to extract information and manipulate with the device
- Normally require expensive equipment, knowledgeable attackers and time
- Destructive, hence, leave evidence of the attack
- Most are irreversible

Semi-invasive attacks (since 2002): advanced imaging, optical probing…

- Semiconductor chip is depackaged, but the passivation layer remains intact
- Fill the gap between non-invasive and invasive types, being both inexpensive and easily repeatable
- Destructive only to the packaging of the chip
- Many are reversible

Semi-invasive attacks

Positioned between non-invasive and invasive attacks

- Less dangerous to target device (decapsulation without penetration)
- Less expensive and easier to setup and repeat than invasive attacks

Tools

- IC soldering/desoldering station
- Simple chemistry lab
- Wire bonding machine
- Signal generator, logic analyzer and oscilloscope
- High-resolution optical microscope
- Special microscopes (laser scanning, infrared etc.)
- UV light sources
- Heating tools
- Scanning electron microscope
- PC with data acquisition board or FPGA prototyping boards

Semi-invasive attacks

What was the reason to define the new attack method?

- Fill the gap between non-invasive and invasive attacks (minutes/hours vs days/weeks, $100…$1000 vs $50K…$500K)
- 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, and they belong to semi-invasive attacks

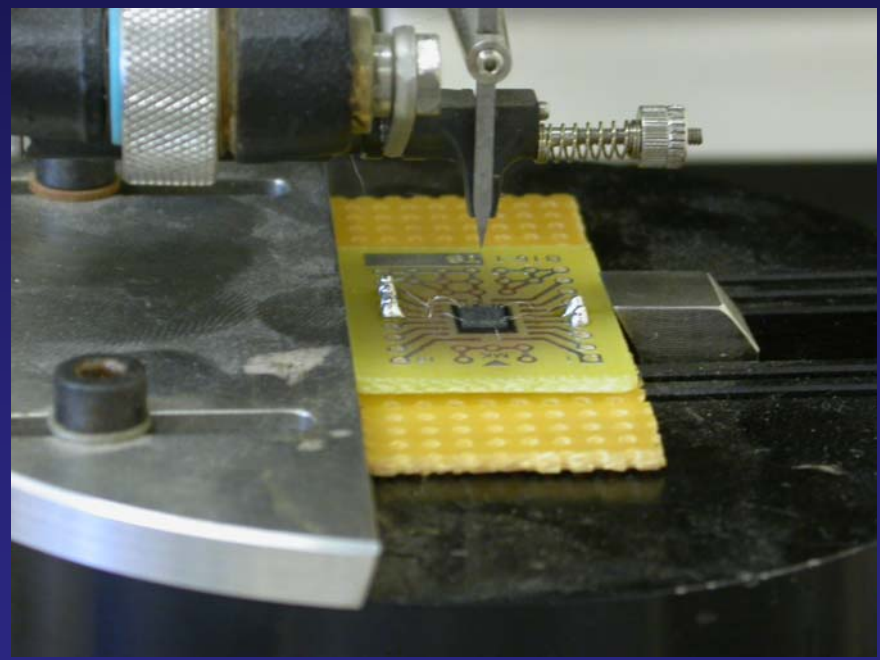
Yet to be explored

- X-rays attacks (without even opening the chip package)
- Interference with strong and localised electromagnetic fields

Semi-invasive attacks

Sample preparation techniques similar to invasive attacks

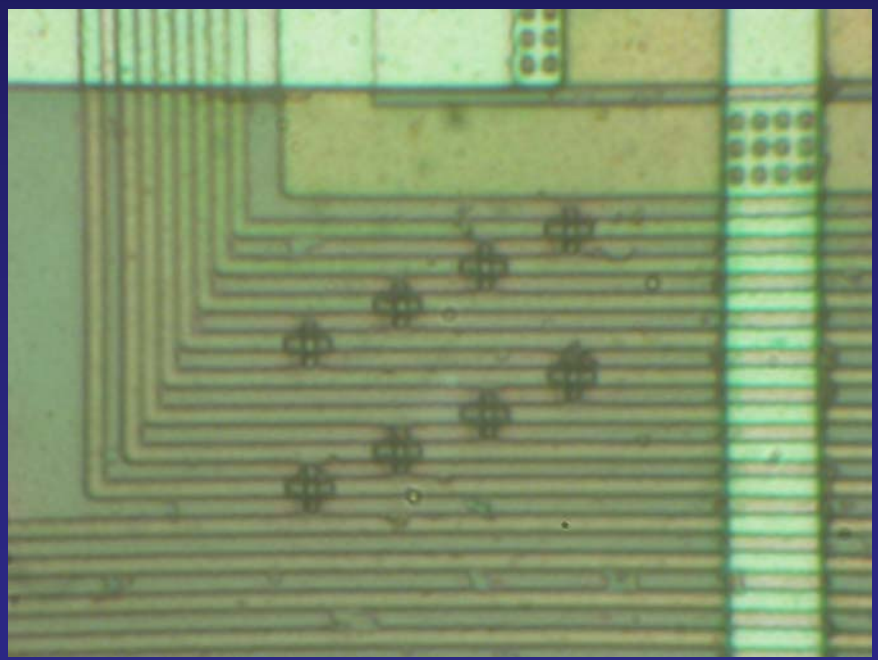
- Decapsulation (front- and rear-side)
- Bonding chips into test packages

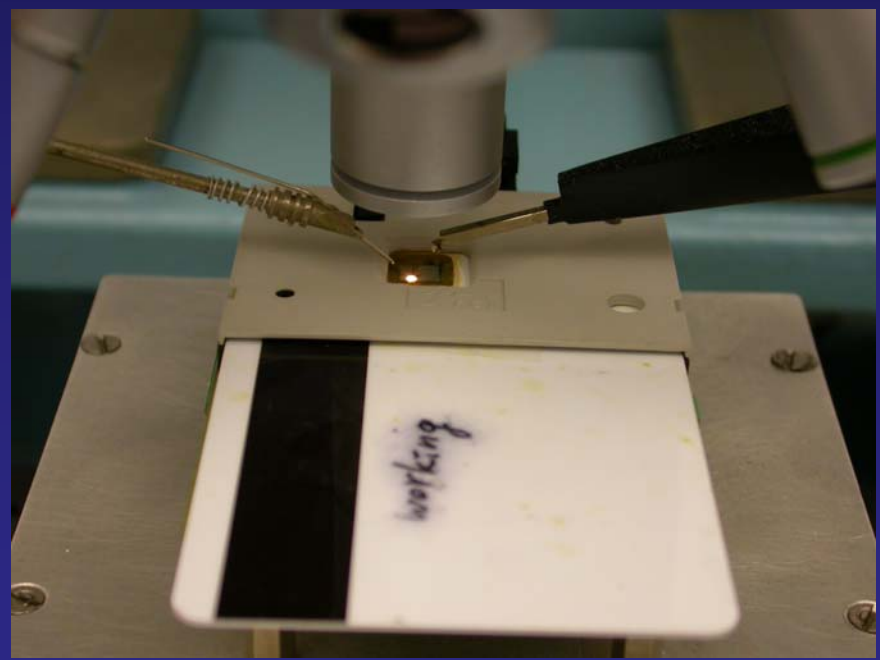


History of semi-invasive attacks

Optical fault injection was observed in my experiments with microprobing attacks in early 2001

- Smartcard sample prepared for invasive microprobing suddenly stopped working when the light inside the microscope was left on
- Further investigations shown that there were no light detectors inside the card

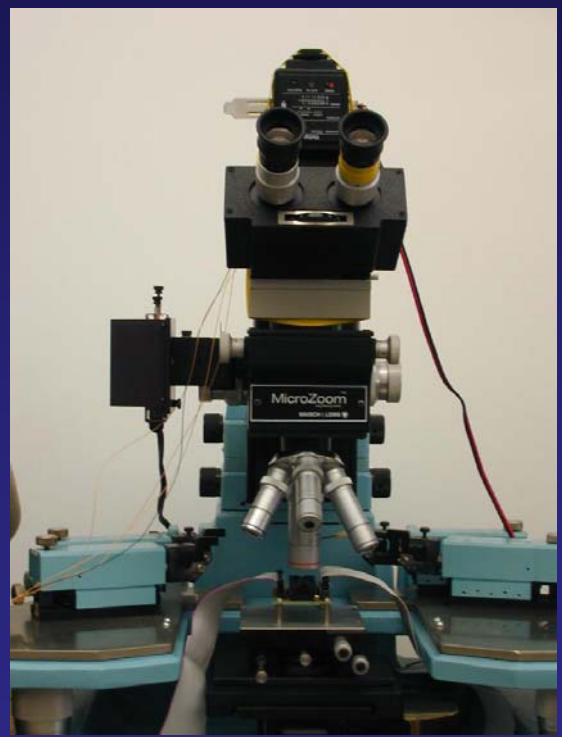




History of semi-invasive attacks

Optical fault injection attacks

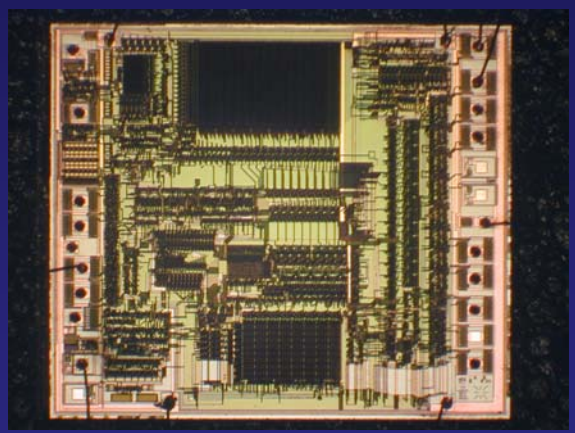
- New class of attacks we introduced in 2002
- Original setup involved optical microscope with a photoflash

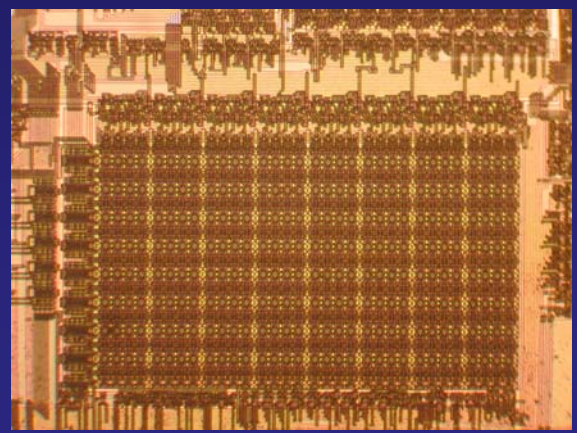


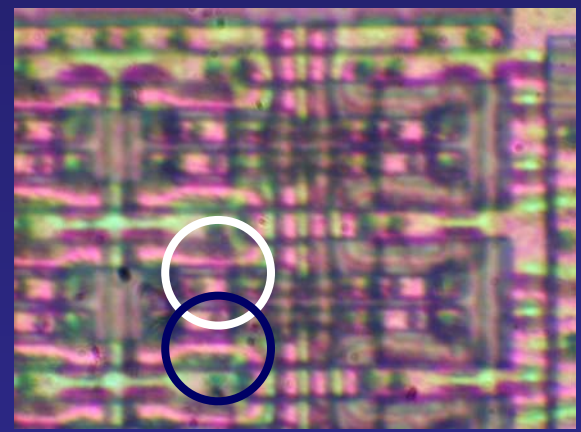
History of semi-invasive attacks

Optical fault injection attack setup

- The Microchip PIC16F84 microcontroller (1.2 μm fabrication process) was programmed to monitor its internal SRAM
- Magnification of the microscope was set to its maximum (1500×)
- Photoflash light was restricted with aluminium foil aperture making it close to parallel and reducing the exposure area on the chip surface



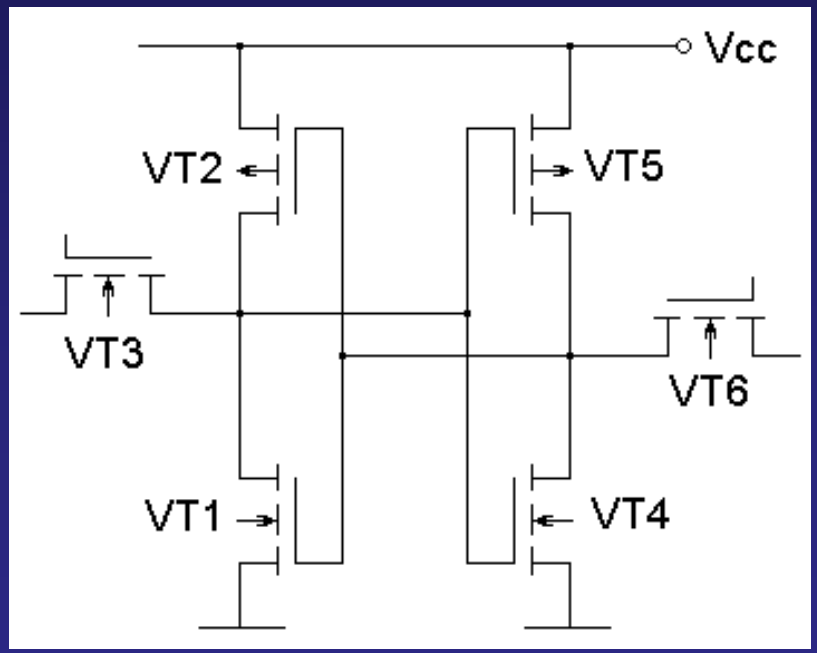


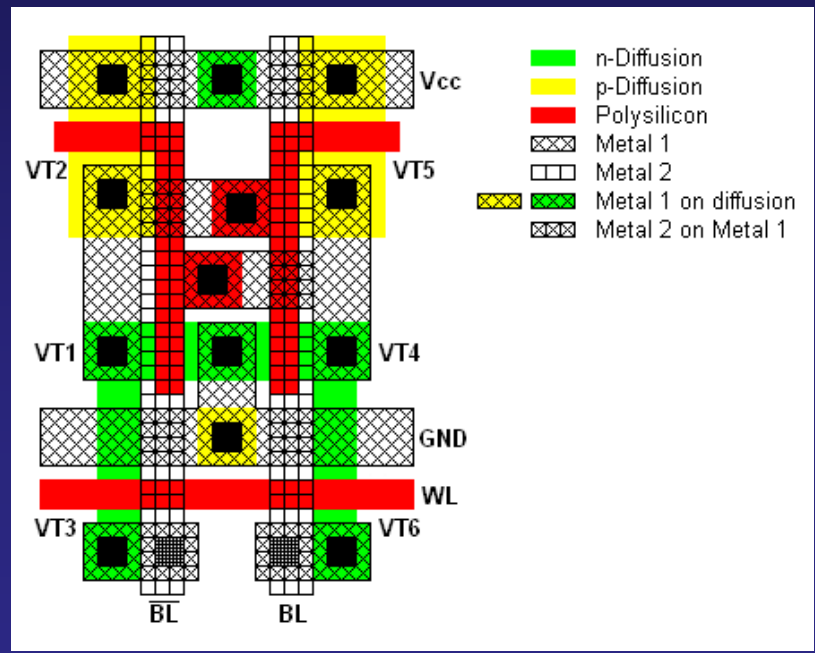


History of semi-invasive attacks

Optical fault injection attacks

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

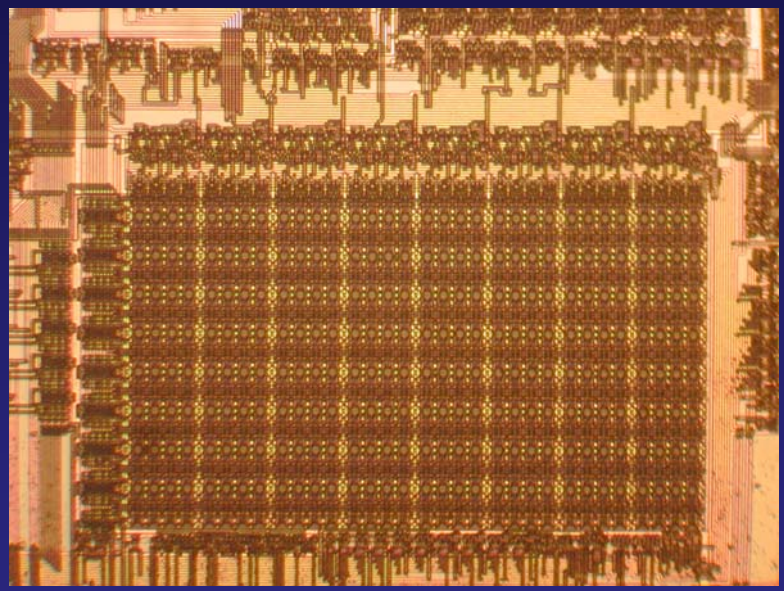




History of semi-invasive attacks

Optical fault injection attacks

- Allocation of memory bits inside the array
- Physical location for each memory address



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

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

Old semi-invasive attacks

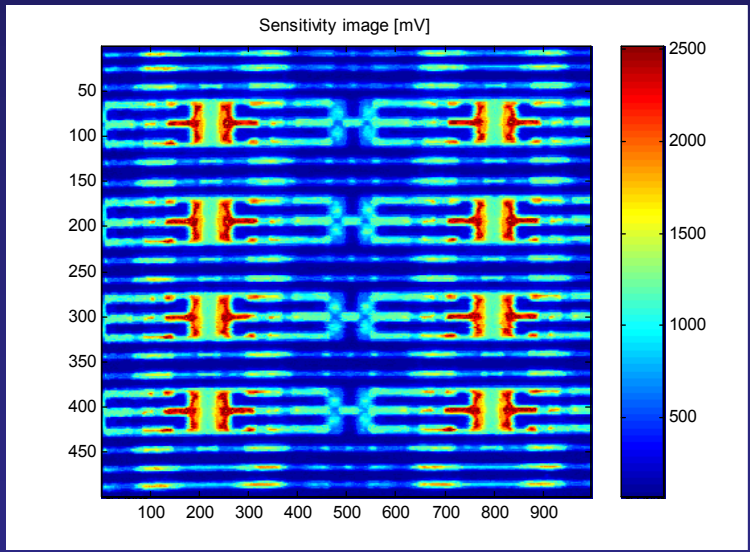
UV attacks

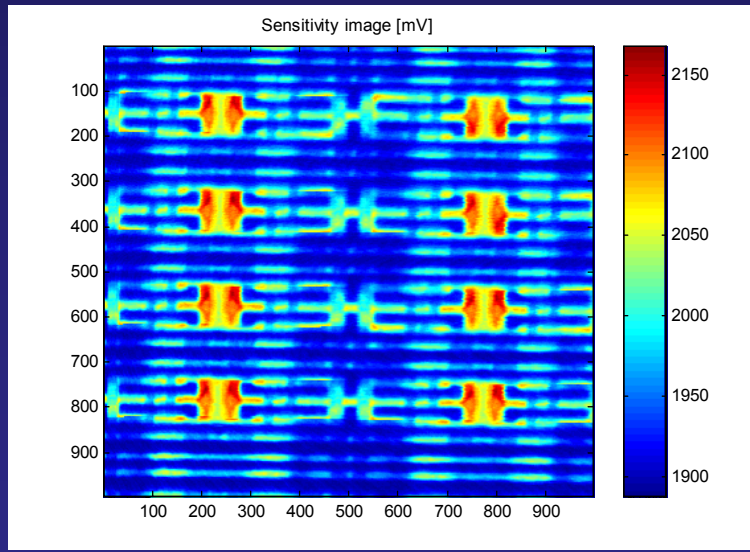
- Well known for over 20 years and used for EPROM and EEPROM
- Usually do not work on chips fabricated with 0.35 µm or smaller process
  - Multiple metal layers block >95% of the active area
  - CMP process used in fabrication of modern chips diffuses the light
- Not suitable for most Flash devices
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

Reading logic state of CMOS transistors

Advanced imaging technique – active photon probing

- Change of optical beam induced current (ΔOBIC)
  - 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)
- Application – reading logic state of CMOS transistors and SRAM cells





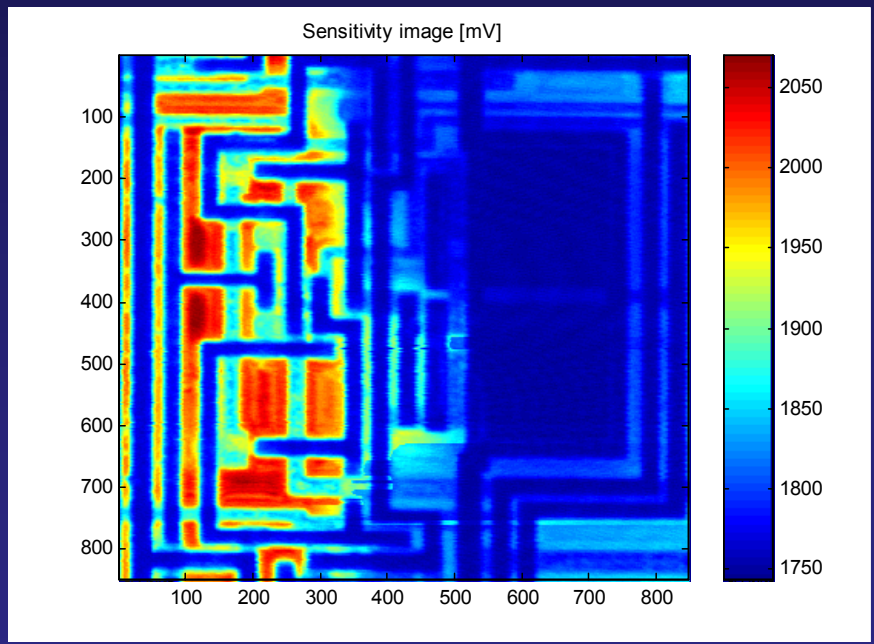
Microchip PIC16F84 microcontroller

Hardware security analysis

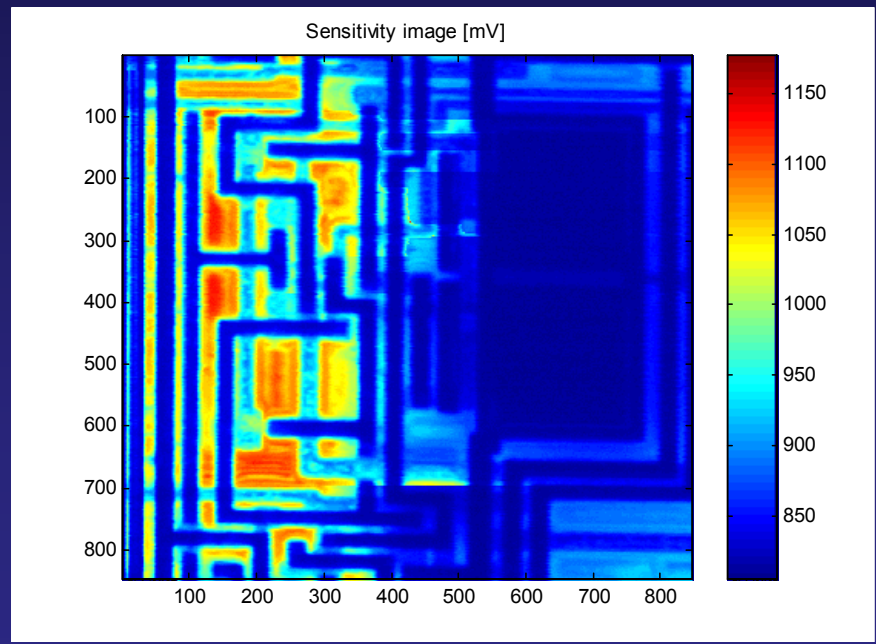
Using semi-invasive imaging techniques to locate security fuses

- Light-induced current variation method
- Comparing two scans – one for non-secure device, other for secure

Non-secure state



Secure state

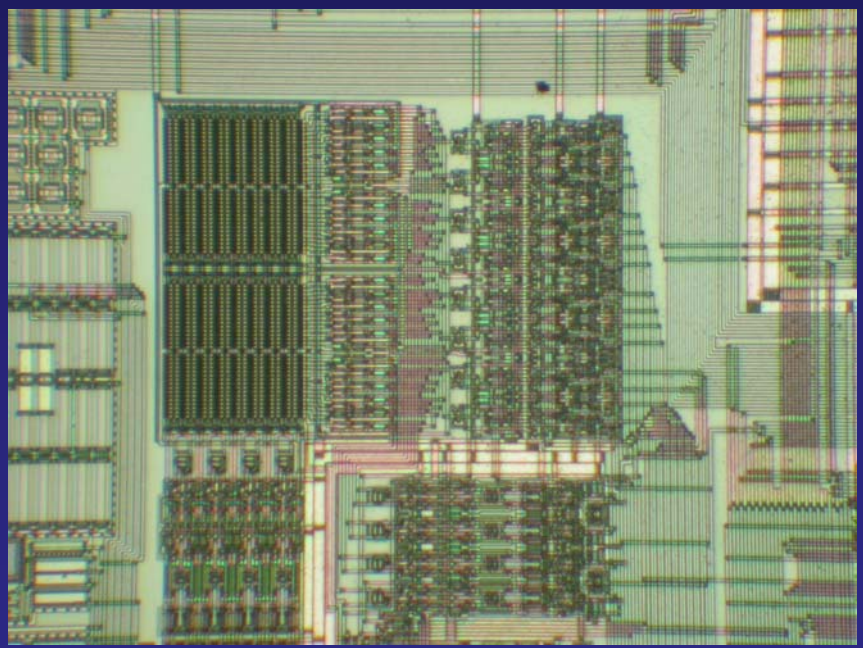


Microchip PIC16F84 microcontroller

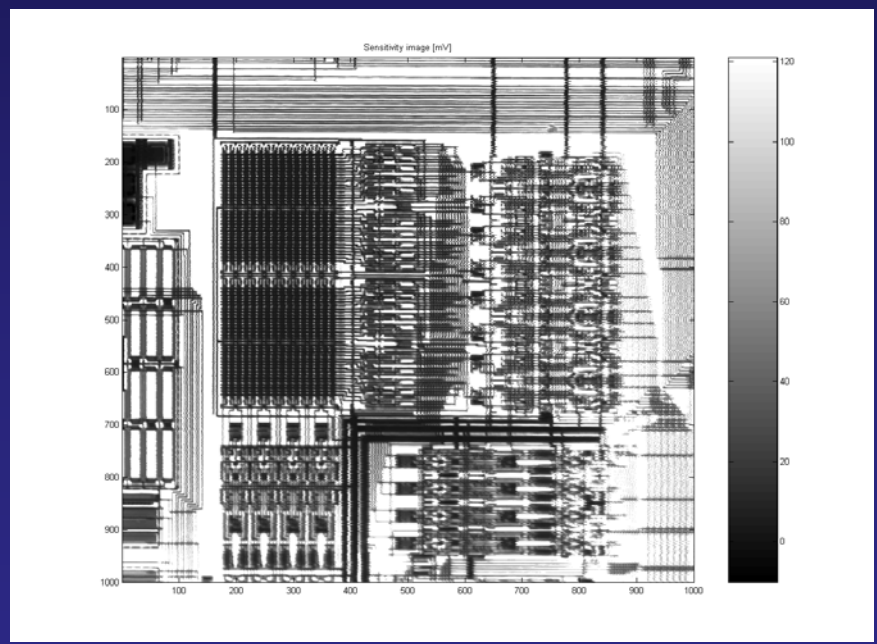
Data remanence in EEPROM and Flash

Residual charge left inside cells in memory devices

- Extracting information from erased memory cells (even after 10 erase cycles)
- Using lasers to
  - monitor the state of memory transistors
  - influence cell characteristics (V_{TH})
  - influence read-sense circuit (V_{ref})



Microchip PIC16F84 microcontroller



Optically Enhanced Power Analysis

A new attack technique I introduced in 2006

Combines

- Power analysis (non-invasive)
- Optical probing (semi-invasive)

Application: Monitoring instructions and data in real time

- What information flows inside the device (data)?
- Where is the information stored (address)?
- What is the result of an operation (conditional branch, flags)?

Advantages

- Isolates individual locations on chip for observation
- Non-destructive
- No interference with device operation
- No modification to memory (EEPROM, SRAM)

A new attack technique

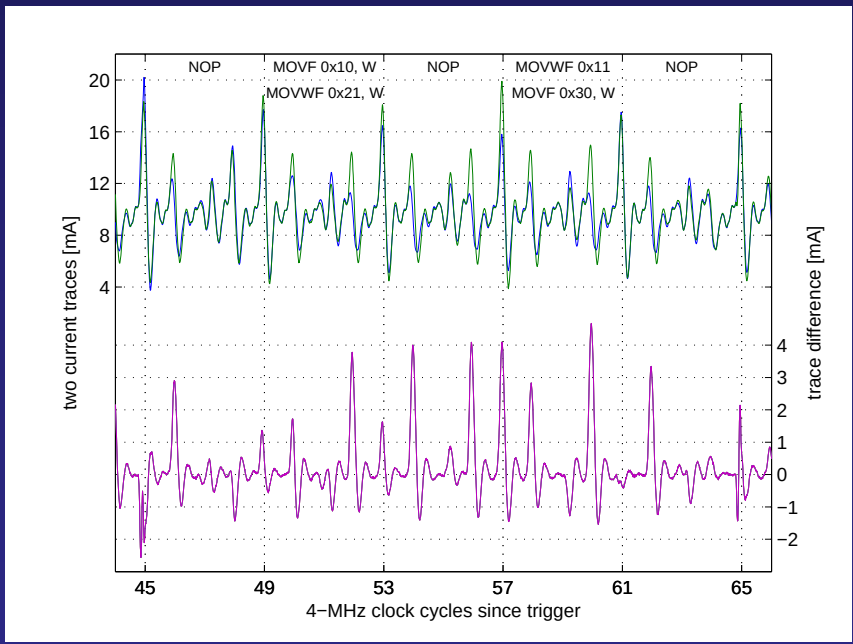
Reasons for developing the new attack technique

- More efficient than existing analysis techniques
  - Power analysis
  - Optical probing
- Faster than invasive attacks (e.g. microprobing)
- Relatively easy to set up
- No modifications required to the semiconductor chip
- Will not interfere with normal device operation

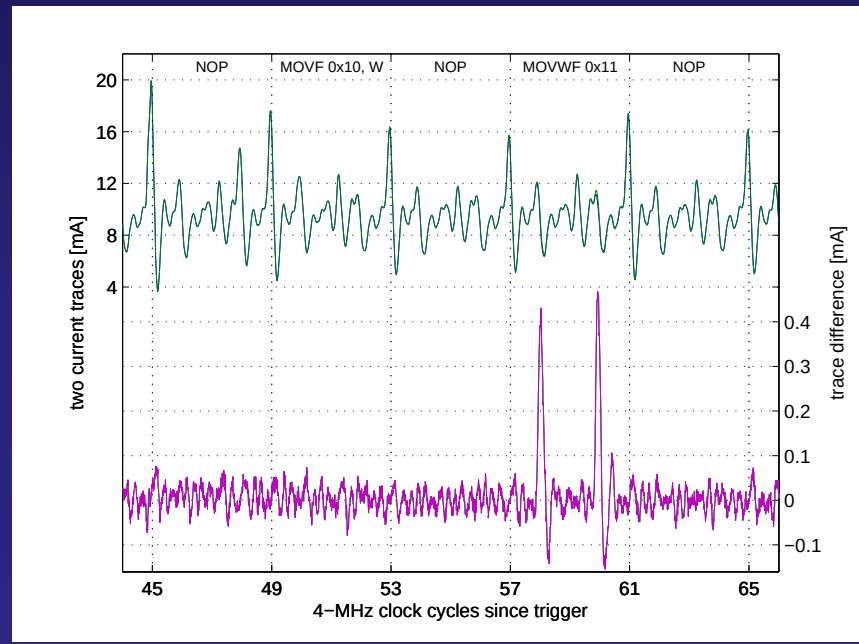
Conventional power analysis

Measuring power consumption during device operation

- Non-invasive attack with a simple setup (resistor & oscilloscope)
- Averaging can be used to reduce noise and increase resolution
- Each CPU instruction has its own waveform
- Different values of data influence on the power trace (lower signal)



PIC16F84: Difference between instructions

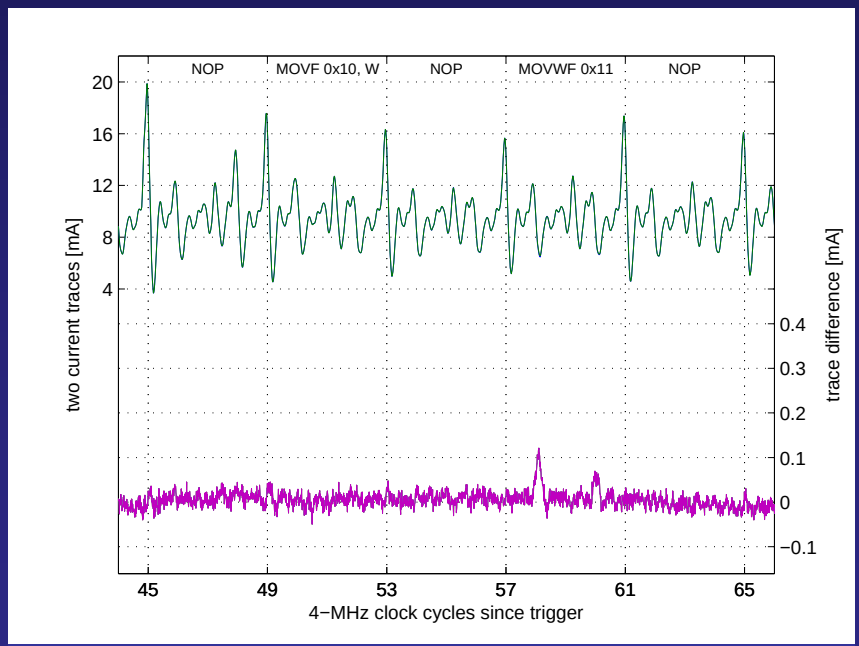


PIC16F84, Write: (0x00 → 0x00) − (0x01 → 0x00) (Av = 64)

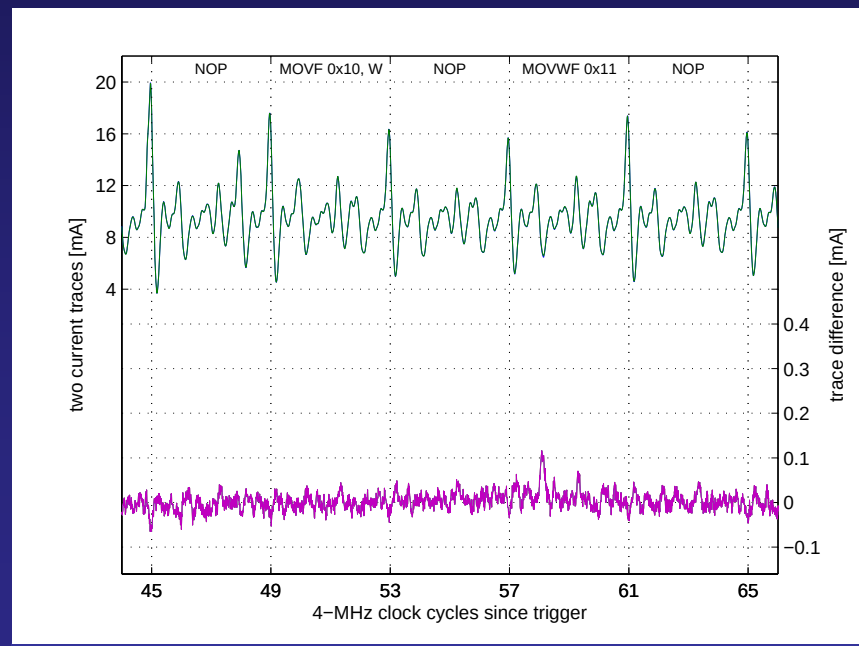
Conventional power analysis

Can we distinguish between 0xD4 and 0x9A data values?

- Very hard to distinguish values with the same Hamming weight
- Sometimes possible if small number of bits has changed
  - For example: 0x01 vs 0x10; 0xF7 vs 0xDF
  - Averaging over a large number of power traces is essential to reduce the noise



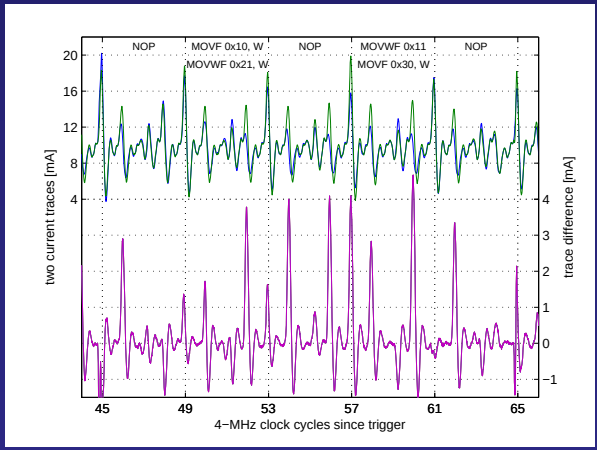
PIC16F84, Write: (0x01 → 0x00) − (0x10 → 0x00) (Av = 256)



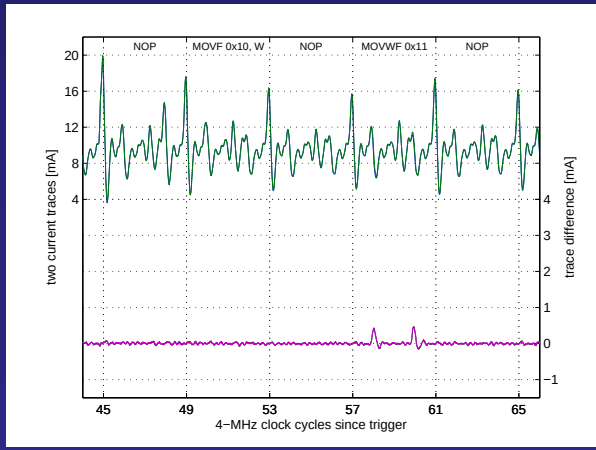
PIC16F84, Write: (0xF7 → 0x00) − (0xDF → 0x00) (Av = 256)

Power analysis summary

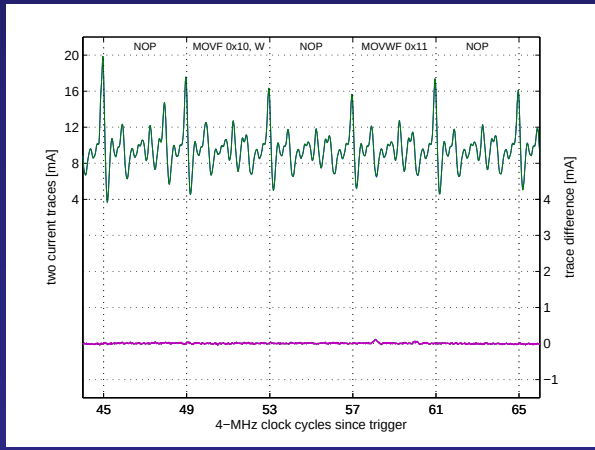
- Non-invasive attack with a simple setup (resistor in power line + oscilloscope)
- Measurements are applied to a whole chip rather than on a small area
- Detects only changes in data values rather than their absolute value
- Averaging is essential to distinguish between small changes in data values, hence longer measurement time
- Data dependency has a tiny contribution in the instruction power trace, Hamming weight dependency has far more less contribution
  - Power ~15 mA, Instructions ~5 mA, Data (1 bit) ~0.5 mA, Hamming weight ~0.05 mA



PIC16F84: Difference between instructions



Write: (0x00→0x00) − (0x01→0x00) (Av = 64)

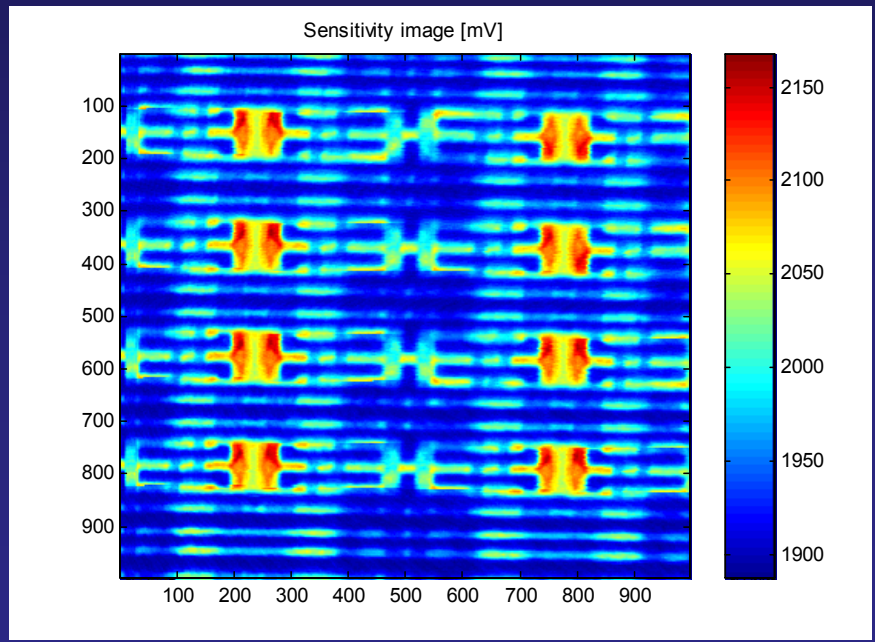


Write: (0x01→0x00) − (0x10→0x00) (Av = 256)

Semi-invasive methods

Use lasers to probe device operation

- Access to the chip surface without mechanical contact
- Widely used in failure analysis of semiconductors (LIVA, TIVA)
  - Determine state of CMOS transistors in static mode
- Direct observation of signals inside a semiconductor (polarization)
  - Expensive setup and special sample preparation
- Modified OBIC (delta OBIC)
  - Measures difference in power consumption
  - Does not change SRAM state
  - Relatively high cost and low sensitivity
- Changes caused by injected photocurrent are very small
  - <0.05 mA vs >0.5 mA in SPA
  - Most techniques are static



Comparing different methods of analysis

Power analysis is effective for data dependency analysis

Optical methods are effective for recovering absolute values of data

	Power analysis (SPA)	LIVA	ΔOBIC
State of SRAM cell	No	Yes	Yes
Access to SRAM cell	Limited	No	Limited
State change of SRAM cell	Yes	No	Limited
Real-time measurement	Yes	No	Limited

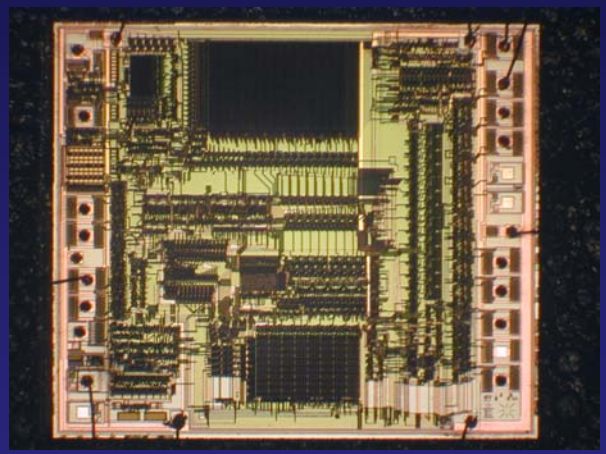
Research questions:

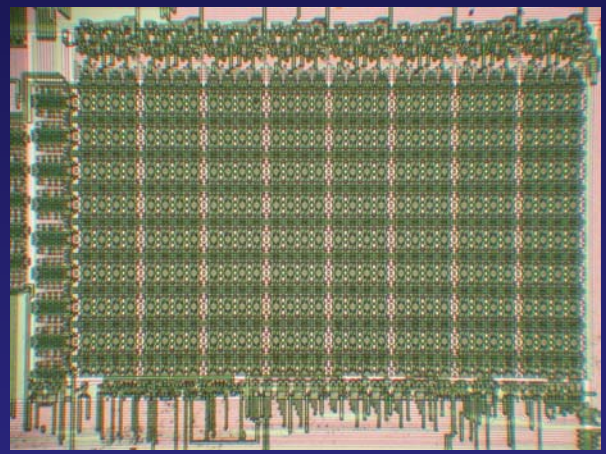
- Is it possible to combine semi-invasive optical probing with non-invasive power analysis methods?
- Can we reliably detect a single bit change without interfering with normal device operation and without averaging of power traces?

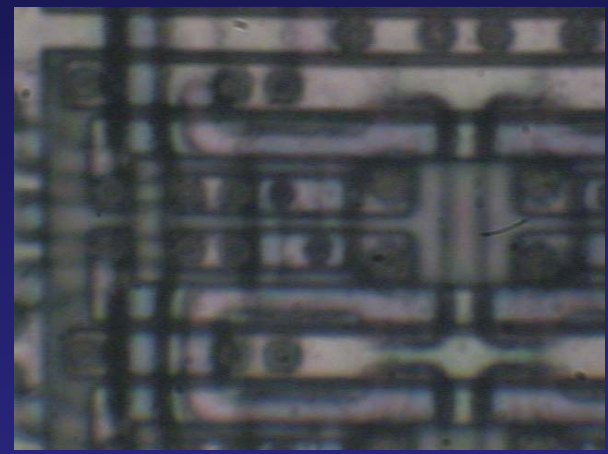
Experimental setup

Target of evaluation: PIC16F84 microcontroller

- Known physical locations for all the SRAM cells (from optical fault injection experiments)
- Known layout of the SRAM cell







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

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

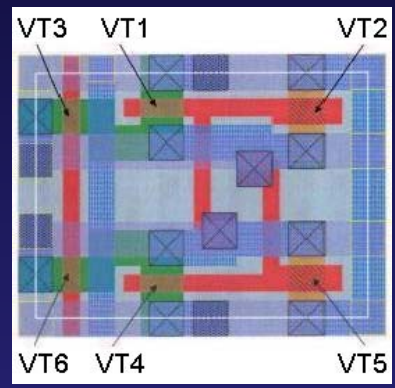
Why an SRAM cell?

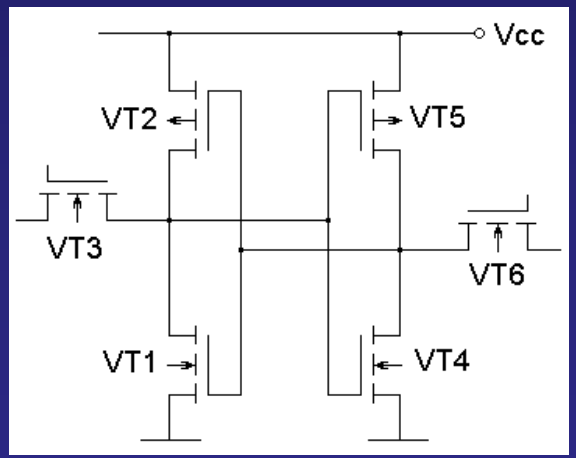
Widely used in modern devices as volatile memory

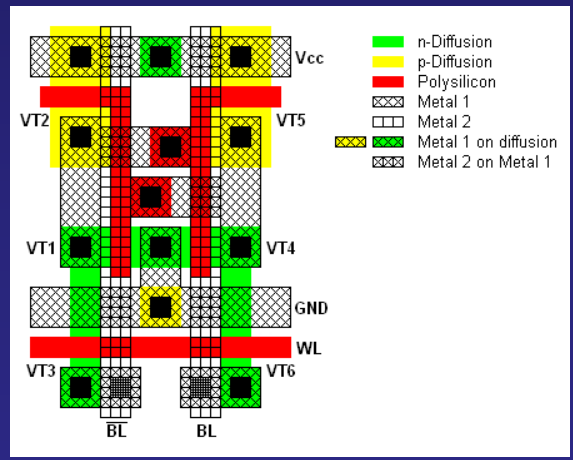
- CPU registers, Data memory, Cache memory

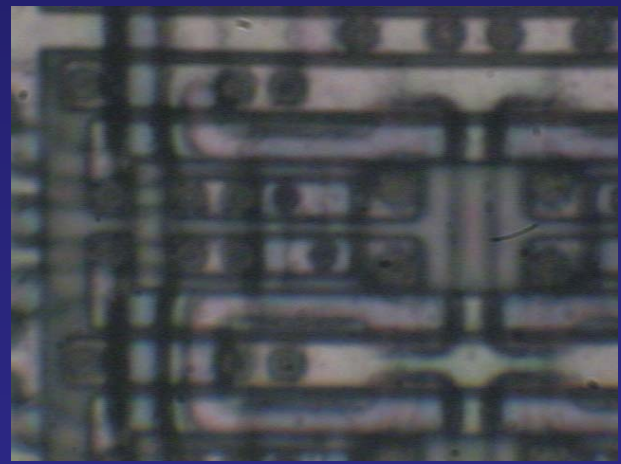
As a result, all cryptographic algorithms and password authentication go through it

- If an attacker gets hold of the data in SRAM or CPU registers, he can easily break the system
- Good for debugging and analysis







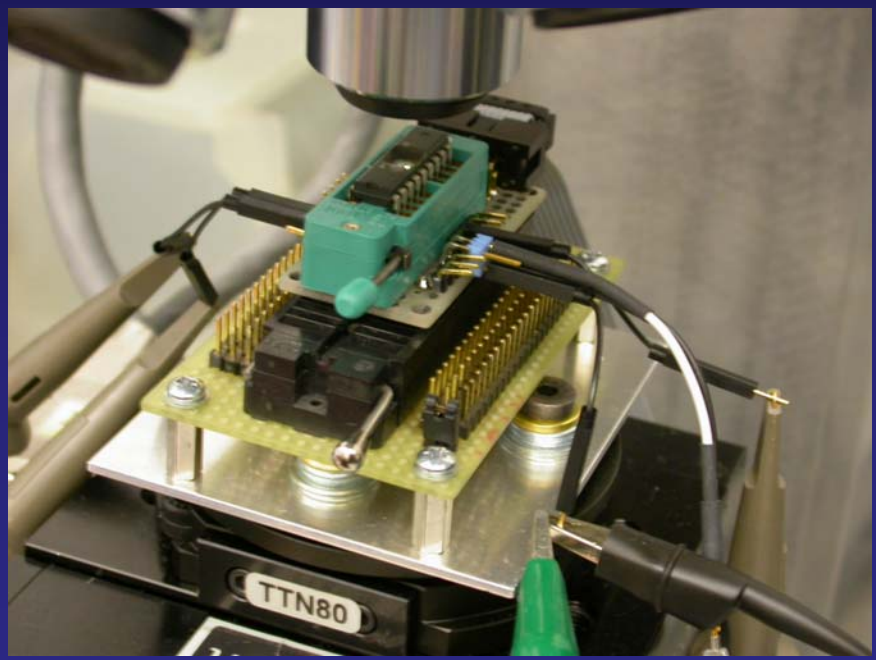


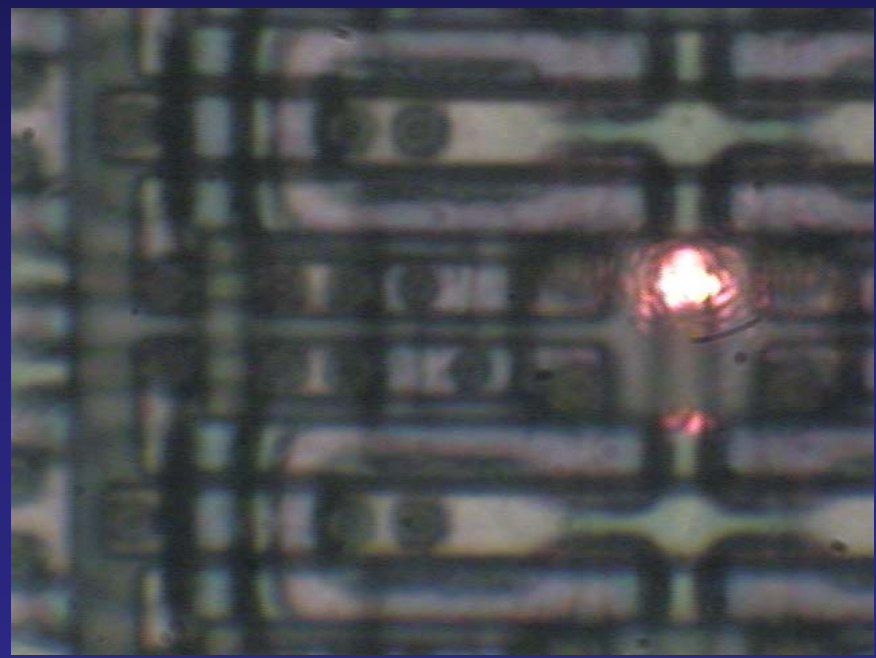
Experimental setup

Decapsulated PIC16F84 on a test socket

Standard power analysis setup with 10 Ω in GND

Laser (639 nm, 0…5 mW) focused using 100× objective

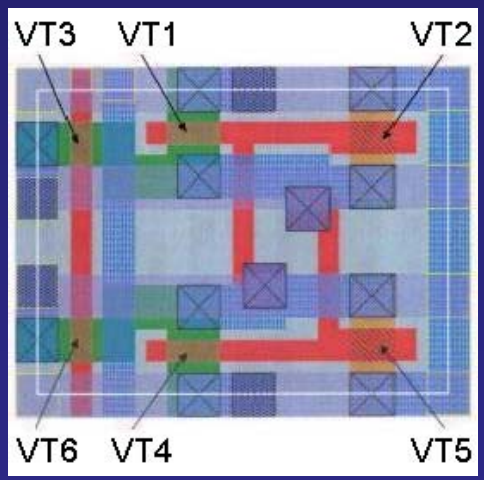


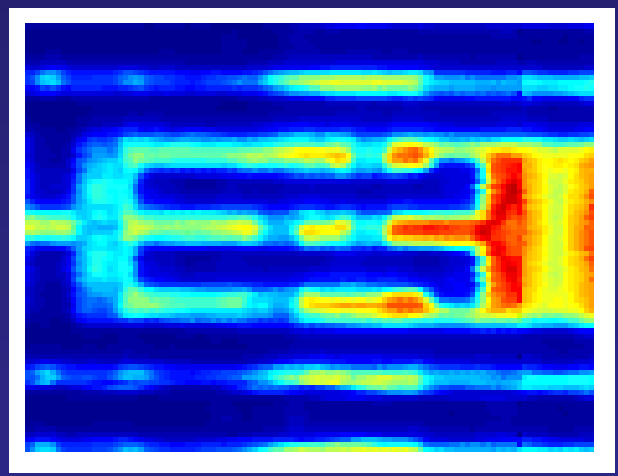


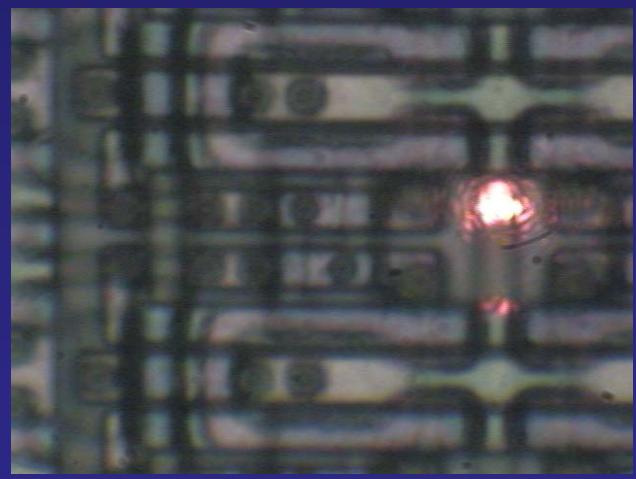
Experimental setup

PIC16F84: Test sequence

- Microcontroller programmed with a test code
  - Generate trigger pulse for oscilloscope
  - Read from the SRAM memory locations
  - Write to the SRAM memory locations
  - Dump SRAM memory for verification
- Known physical location and layout for all SRAM cells
- Light-sensitive locations for VT1…VT6 from OBIC laser scan
- Repeat measurements for different laser positions and power settings



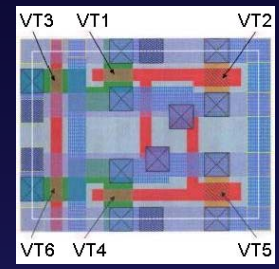


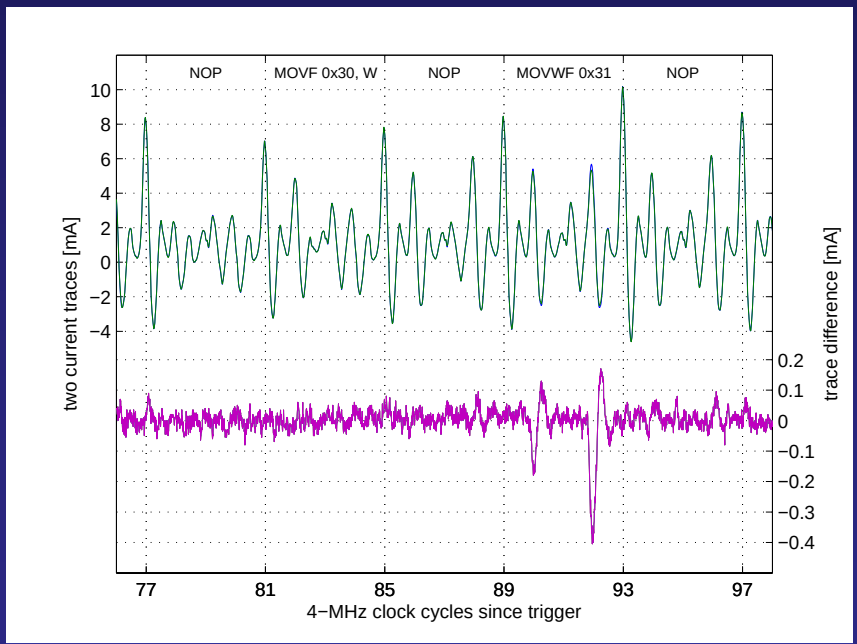


Results

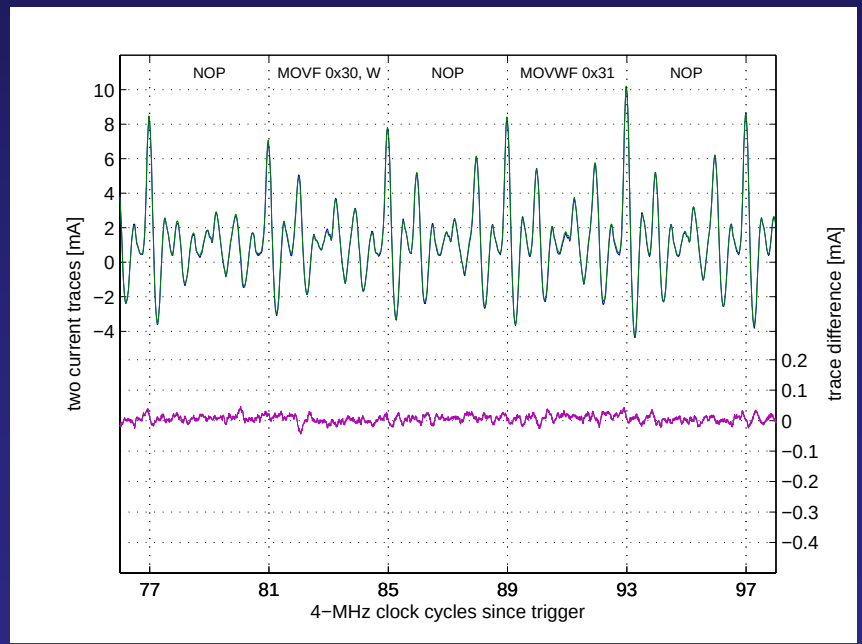
Laser focused on VT1 (n-channel) of the SRAM cell

- State of the cell stays unchanged for low laser power
  - Maximum difference is less than a single-bit change influence
  - Only writing into the memory cell can be detected (address 0x31)
- The result is very similar to ΔOBIC observation, but dynamic





PIC16F84, Write: (0x00 → 0xFF) − (0x00 → 0xFF)$_L$ (Av = 16)

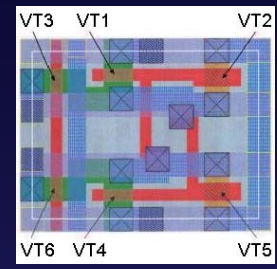


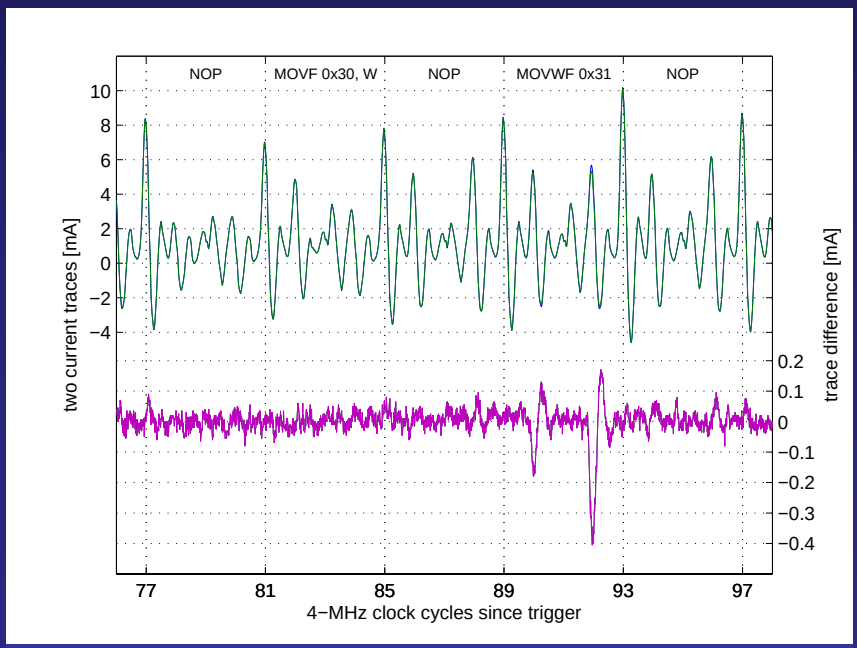
PIC16F84, Read: (0xFF) − (0xFF)$_L$ (Av = 256)

Results

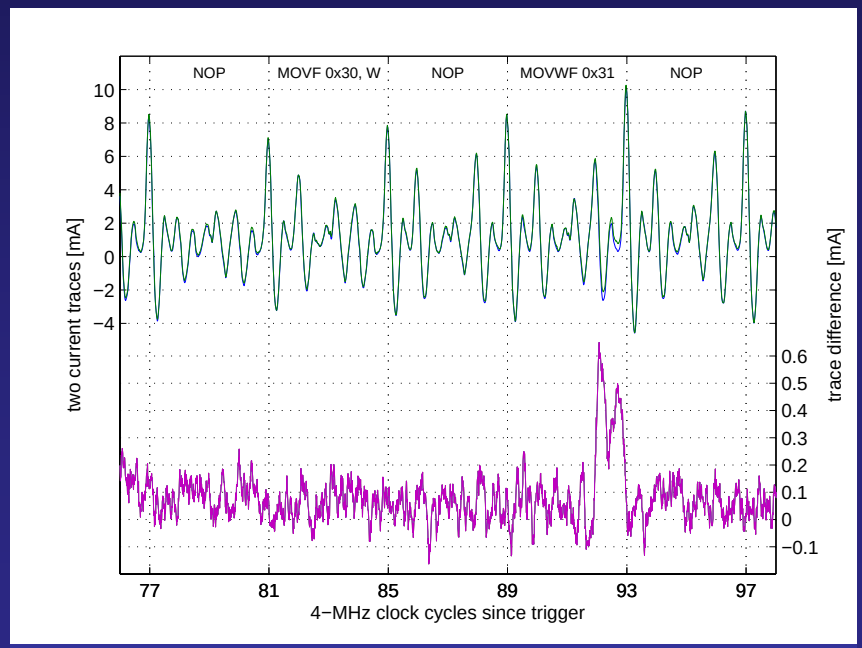
Optimisation for the laser focused on VT1 results

- Increasing the laser power
- State of the cell changes with higher laser power
  - Higher difference than a single-bit change influence (state changing plus injected photocurrent)
  - Both write and read operations can be detected (the data value has changed)





PIC16F84, Write: (0x00 → 0xFF) − (0x00 → 0xFF)$_L$ (Av = 16)

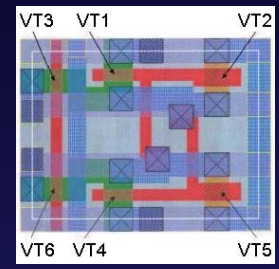


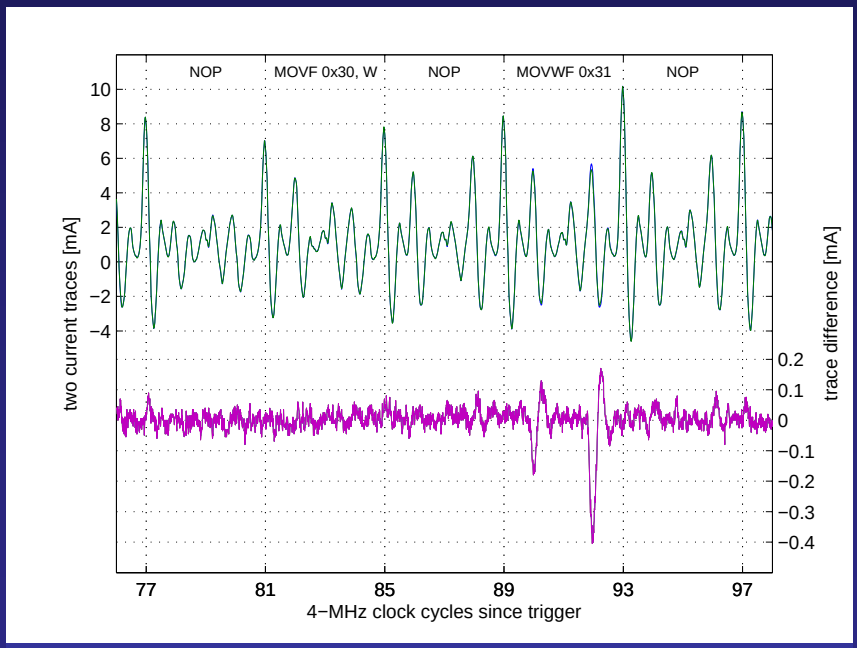
PIC16F84, Write: (0x00 → 0xFF) − (0x00 → 0x7F)$_L$ (Av = 1)

Further improvements to the results

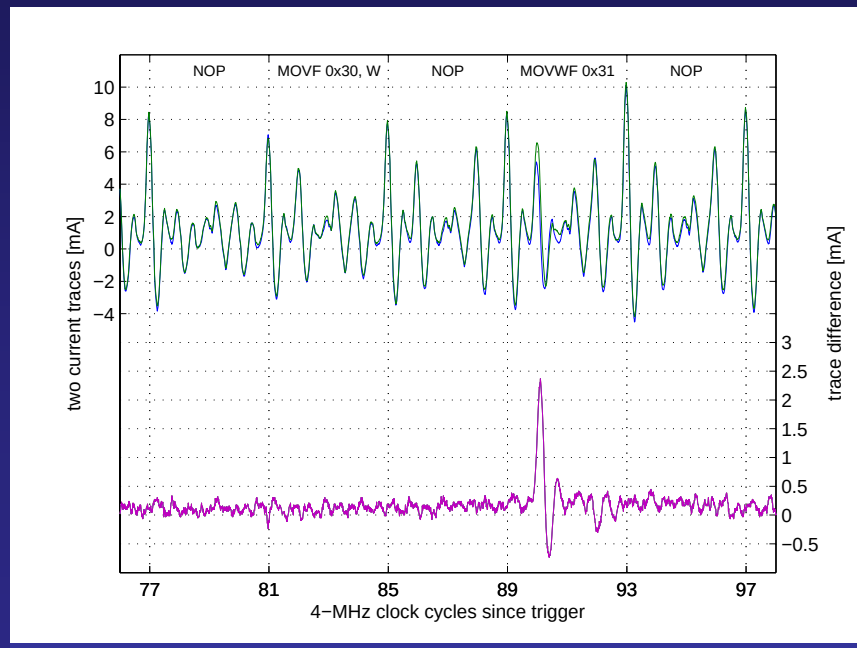
Laser focused on VT1+VT4 of the SRAM cell

- State of the cell stays unchanged for low laser power
  - Response is five times higher than a single-bit change influence
  - No averaging is necessary for reliable detection of the memory-write event





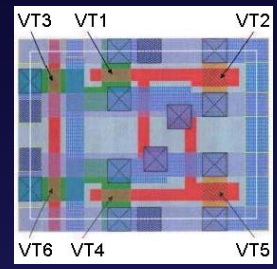
PIC16F84, Write: (0x00 → 0xFF) − $(0x00 \rightarrow 0xFF)_L$ (Av = 16)



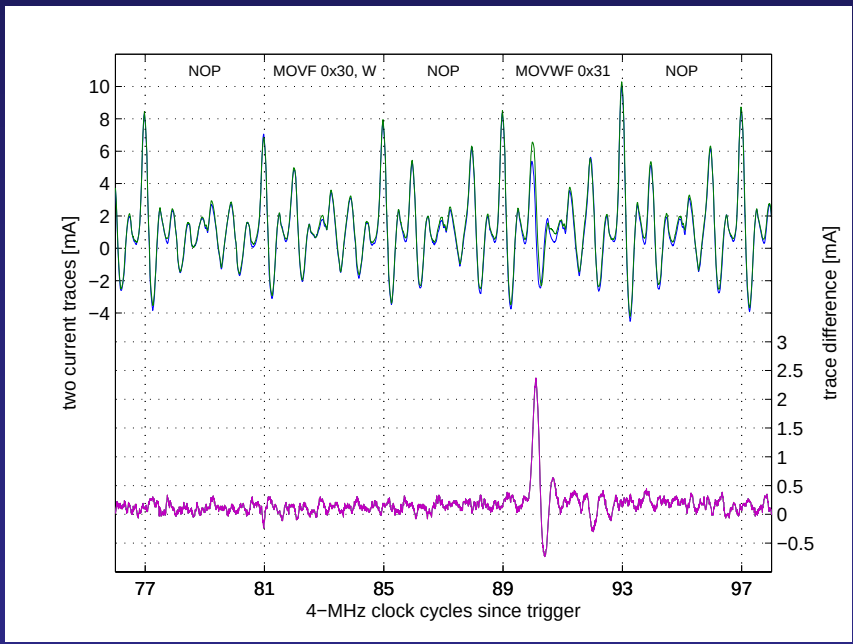
PIC16F84, Write: (0x00 → 0xFF) − $(0x00 \rightarrow 0xFF)_L$ (Av = 1)

Results

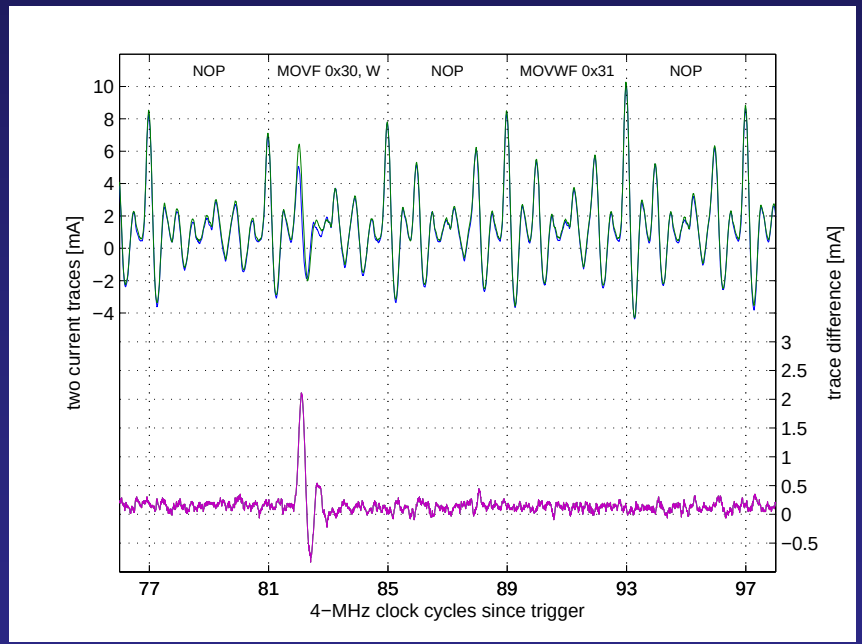
Laser focused on VT1+VT4 (n-channels) of memory cell



- State of the cell stays unchanged for low laser power
  - Both read and write operations can be detected
  - Response is high for both read and write events
- Any access to a particular memory cell is visible in the power trace independently of whether the cell changes its state or not



PIC16F84, Write: (0x00 → 0xFF) − (0x00 → 0xFF)$_L$ (Av = 1)

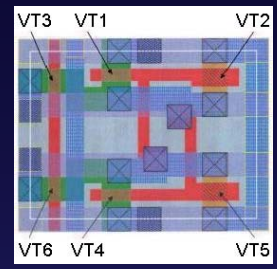


PIC16F84, Read: (0xFF) − (0xFF)$_L$ (Av = 1)

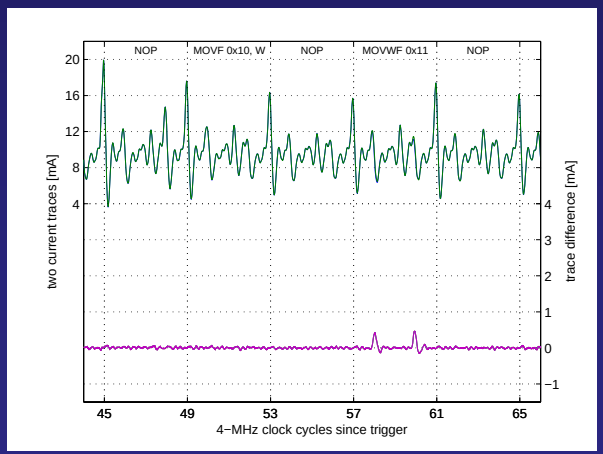
Explaining the results

Why such a high response with the laser on VT1+VT4?

- Compared to single-bit difference in data: 5 times higher
- Compared to the laser on VT1 results: 6…10 times higher

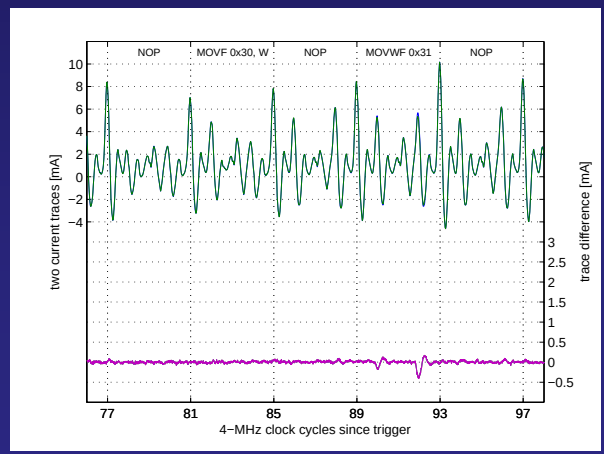


Power analysis result: 1-bit difference



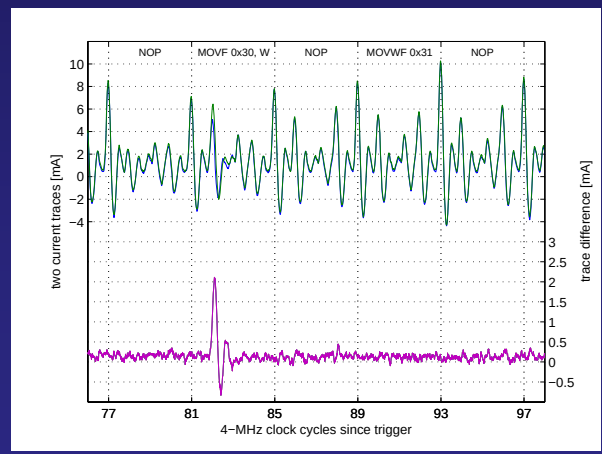
Write: (0x00→0x00) − (0x01→0x00) (Av = 64)

Laser focused on VT1



Write: (0x00→0xFF) − (0x00→0xFF)$_L$ (Av=16)

Laser focused on VT1+VT4

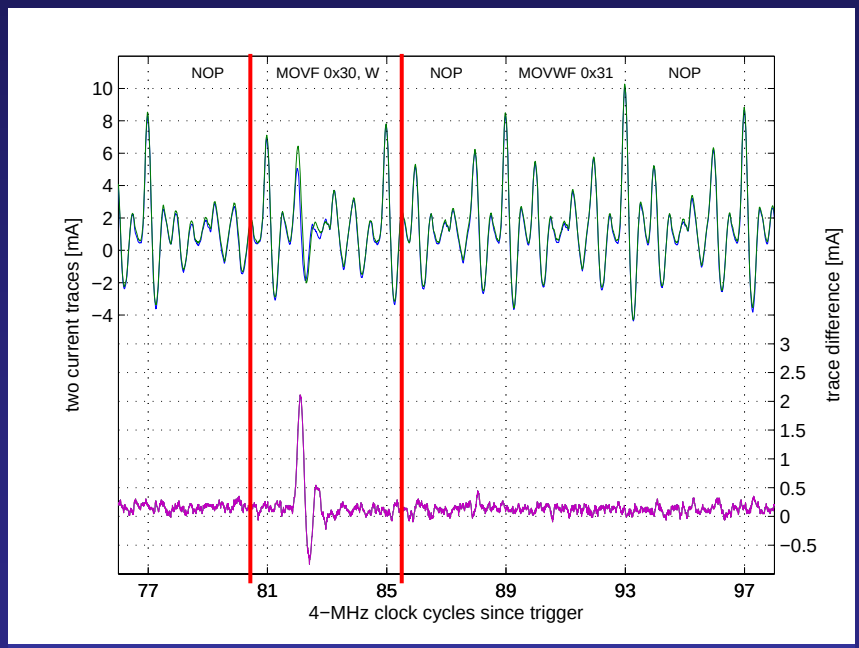


PIC16F84, Read: (0xFF) − (0xFF)$_L$ (Av = 1)

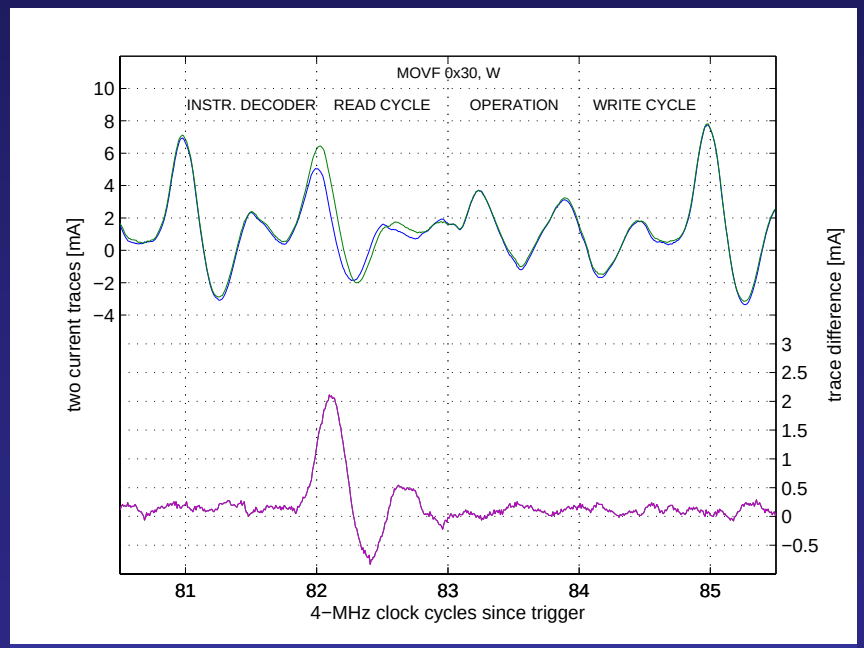
Explaining the results

Characteristics of the SRAM cell are changing when both n-channel transistors (VT1+VT4) of the flip-flop are influenced

- As both CMOS inverters forming the flip-flop become open, a large power surge takes place
- Slower response from the SRAM cell causes a phase shift in the power trace increasing the difference in the power trace



PIC16F84, Read: (0XFF) − $(0xFF)_L$ (Av = 1)

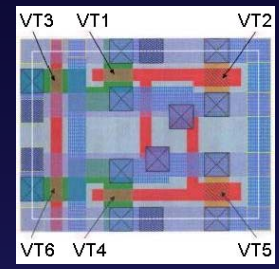


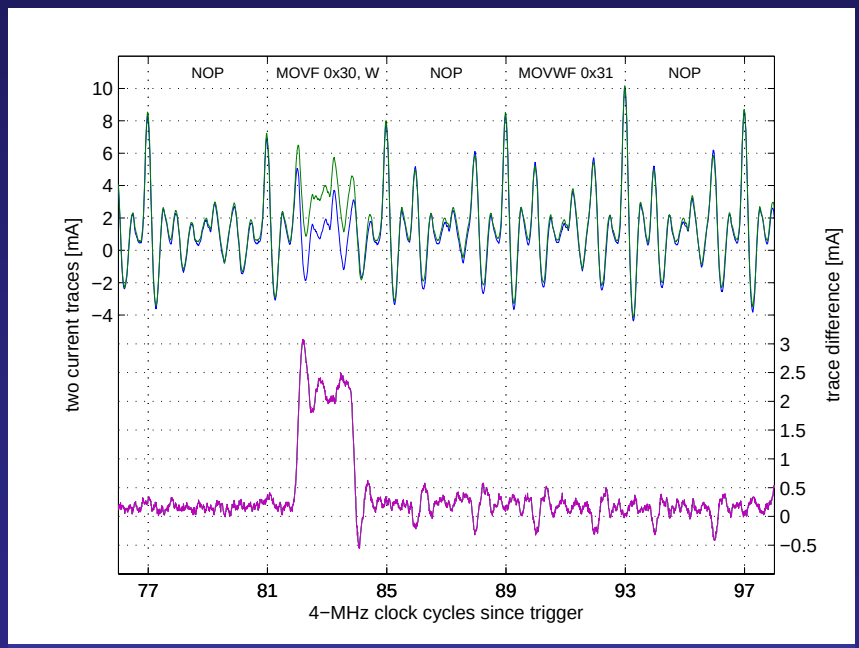
PIC16F84, Read: (0xFF) − $(0xFF)_L$ (Av = 1), ZOOM IN

Applications for higher laser power

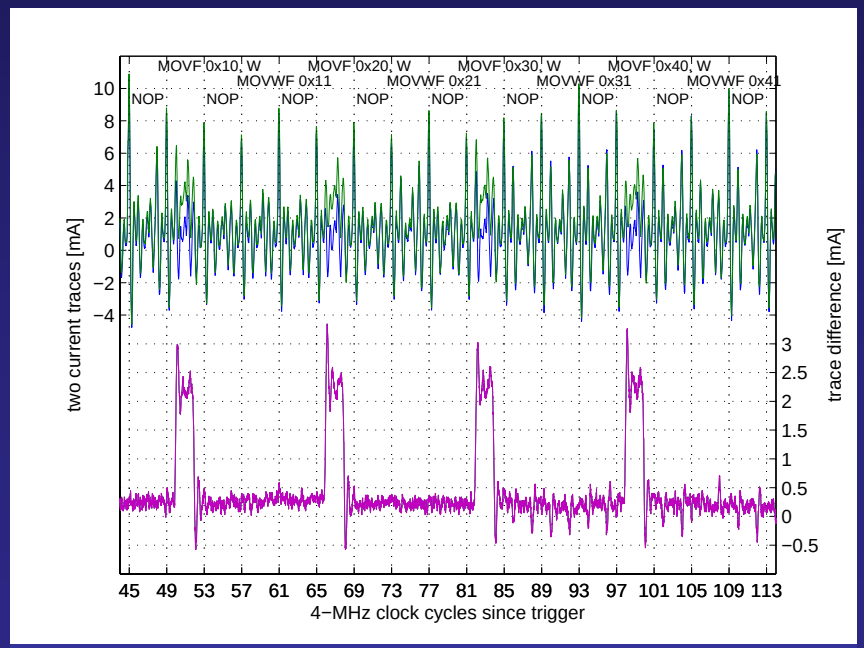
State of the memory cell is likely to change

- Any access to a chosen cell can be detected (VT1+VT4)
- If the laser is focused on VT3+VT6 (select transistors)
  - Read and write operations for any cell in the whole column can be detected
- Can be used for triggering, but affects the normal chip operation





PIC16F84, Read: (0xFF) − $(0xFF)_L$ (Av = 1)



PIC16F84, Read: $(0x00, 0xFF)_L$ (Av = 1)

Comparing different methods of analysis

Optically enhanced position-locked power analysis allows detection of the access event for chosen SRAM cell

It complements and improves the standard power analysis technique allowing to detect the state of a memory cell and providing higher signal-to-noise ratio

It complements optical probing with event detection ability without interfering with the device operation

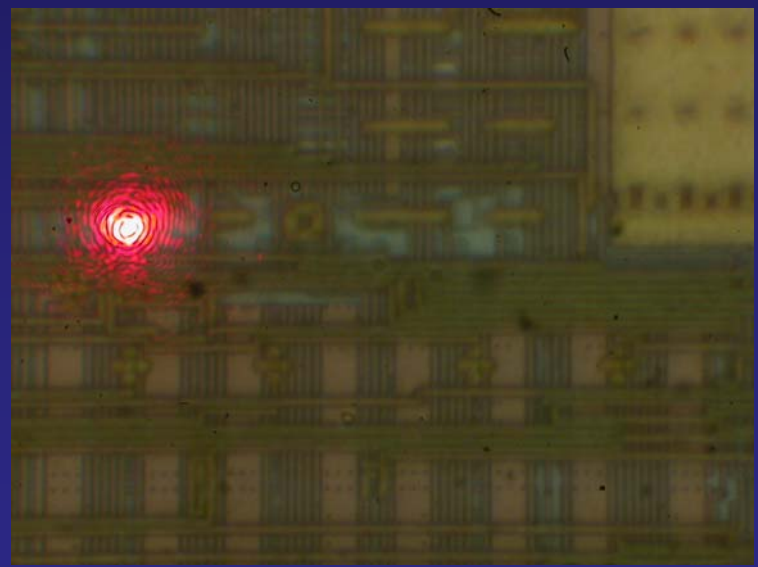
For most applications averaging is not required

	SPA	LIVA	ΔOBIC	OEPA
State of SRAM cell	No	Yes	Yes	Yes
Access to SRAM cell	Limited	No	Limited	Yes
State change of SRAM cell	Yes	No	Limited	Yes
Real-time measurement	Yes	No	Limited	Yes

Semi-invasive attacks

Are there any problems with semi-invasive methods?

- Modern multilayer technologies (0.35 µm or smaller process)
  - Up to 4 metal layers in 0.35 µm technology
  - Up to 6 metal layers in 0.18 µm technology
  - Up to 9 metal layers in 90 nm technology
- Polished layers are less transparent to the light
- Wide top metal layers cover most of the surface (power supply lines)

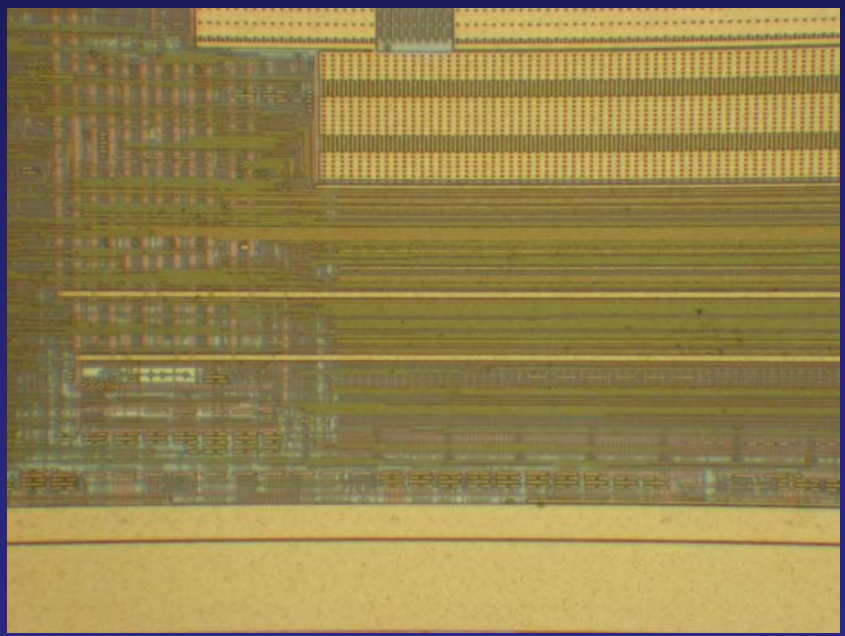


Atmel ATmega8 microcontroller

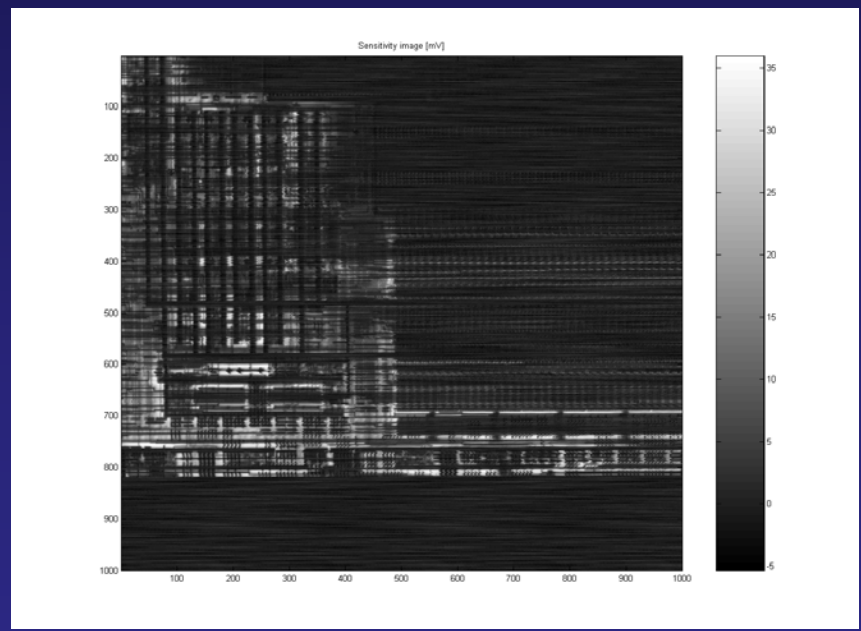
Semi-invasive attacks

Modern multilayer technologies (0.35 µm or smaller process)

- Multiple metal layers plus CMP makes it harder to attack the chip from its front side
- Laser scanning (OBIC) is not very informative
- Optical attacks require higher energy and less precise



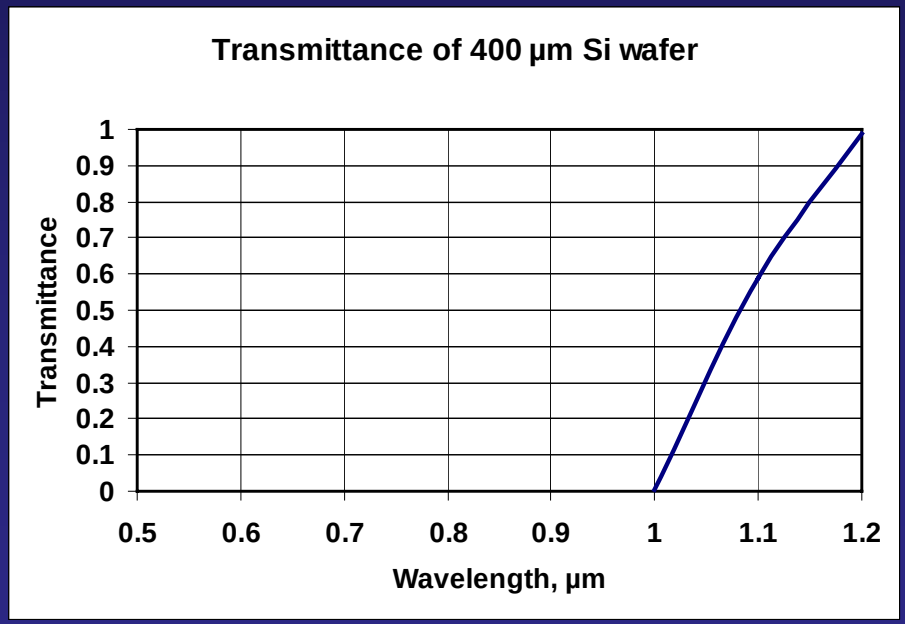
Atmel ATmega8 microcontroller



Semi-invasive imaging techniques

Advanced imaging techniques

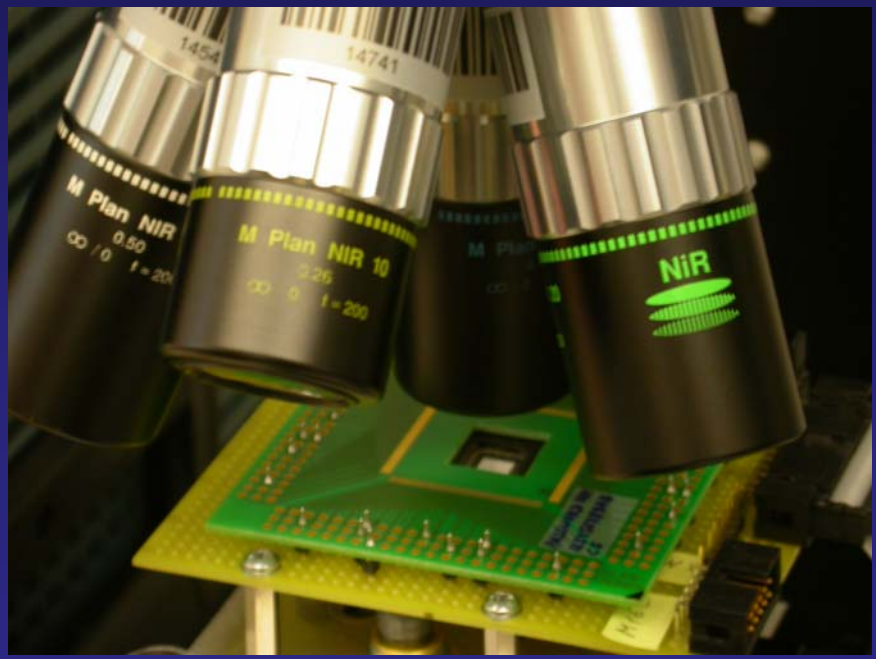
- Approaching chip from rear side with infrared light
- Silicon is almost transparent to photons with $\lambda > 1100$ nm



Semi-invasive imaging techniques

Backside infrared imaging

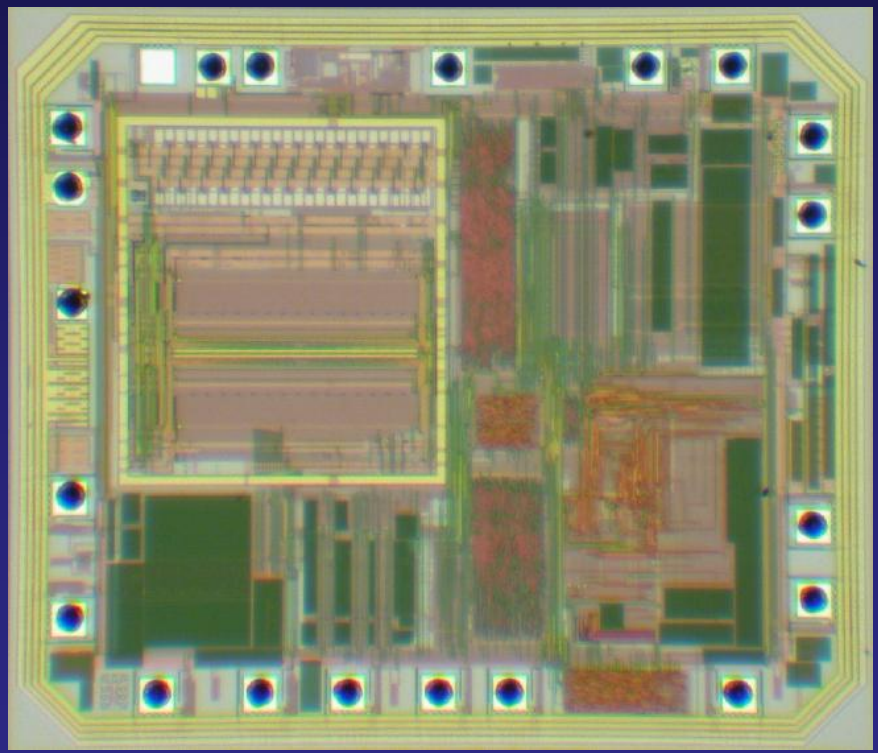
- Microscopes with IR optics should be used
- IR enhanced CCD cameras or special cameras must be used
- Resolution is limited to 0.6 µm by the wavelength of used IR light

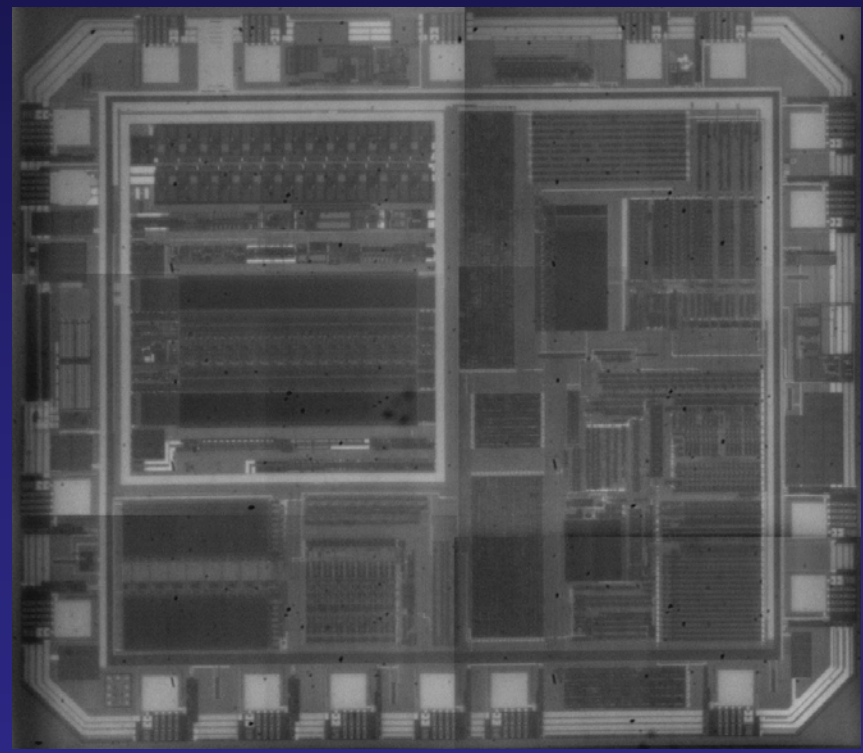


Semi-invasive imaging techniques

Backside infrared imaging

- Reflected and transmitted light illumination can be used



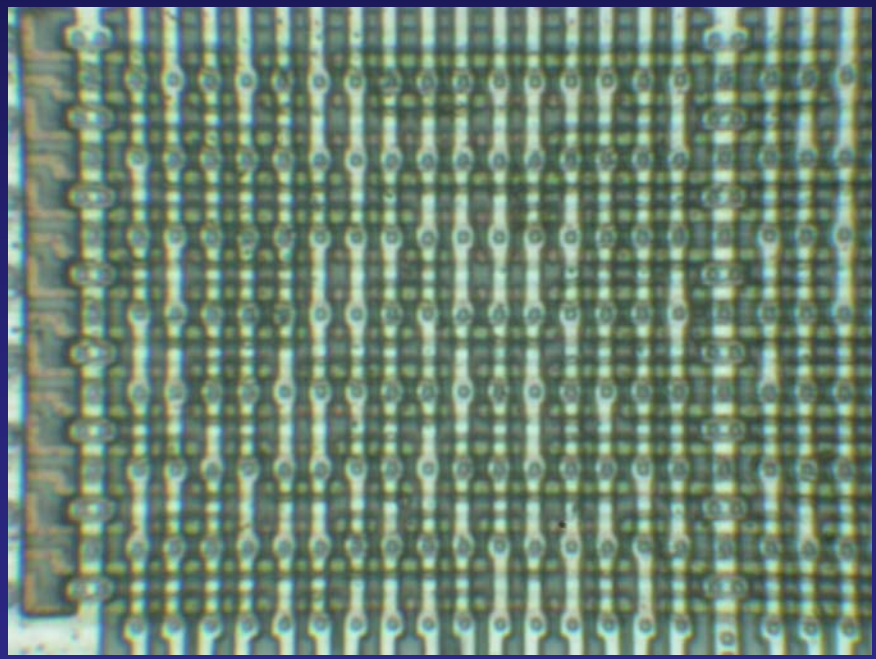


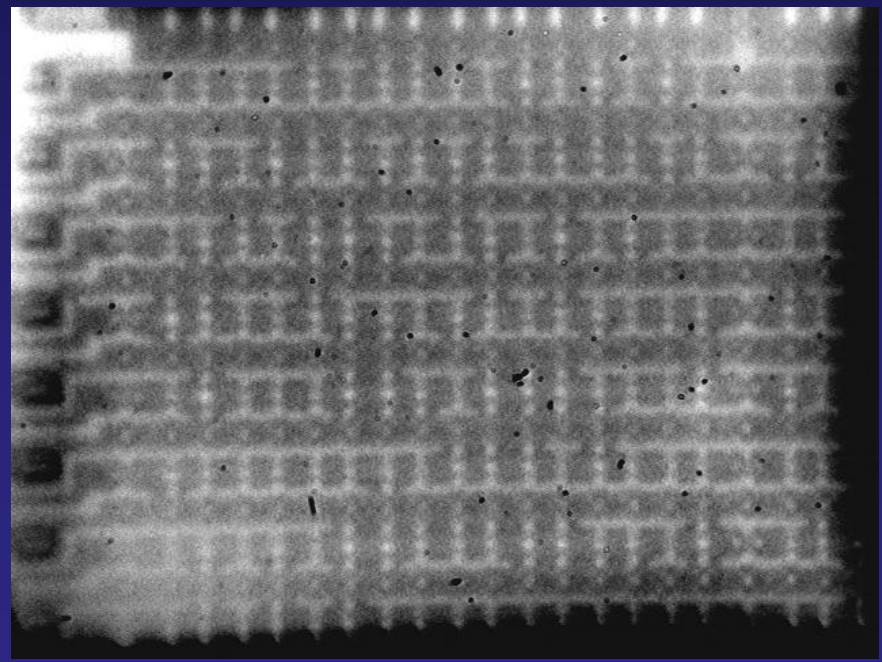
Texas Instruments MSP430F112 microcontroller

Semi-invasive imaging techniques

Backside infrared imaging

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



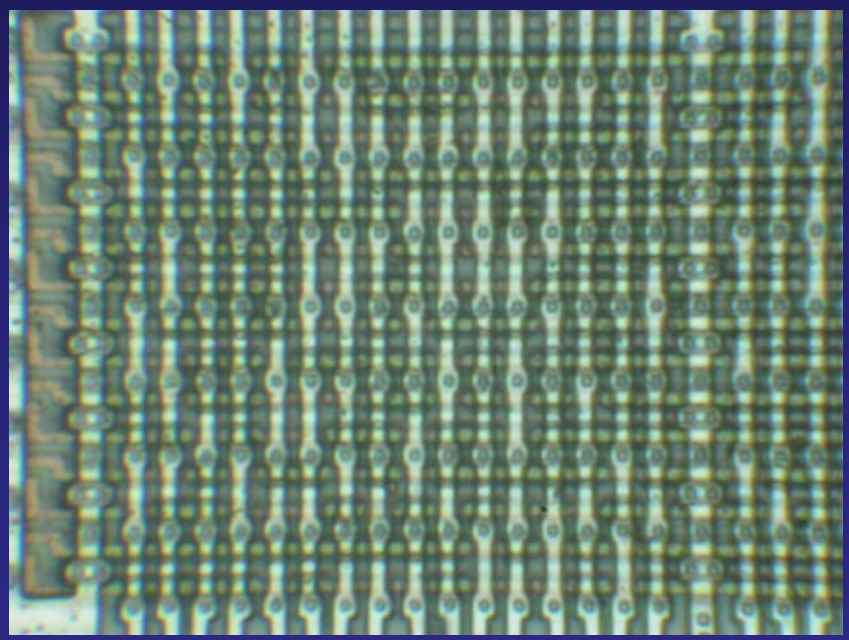


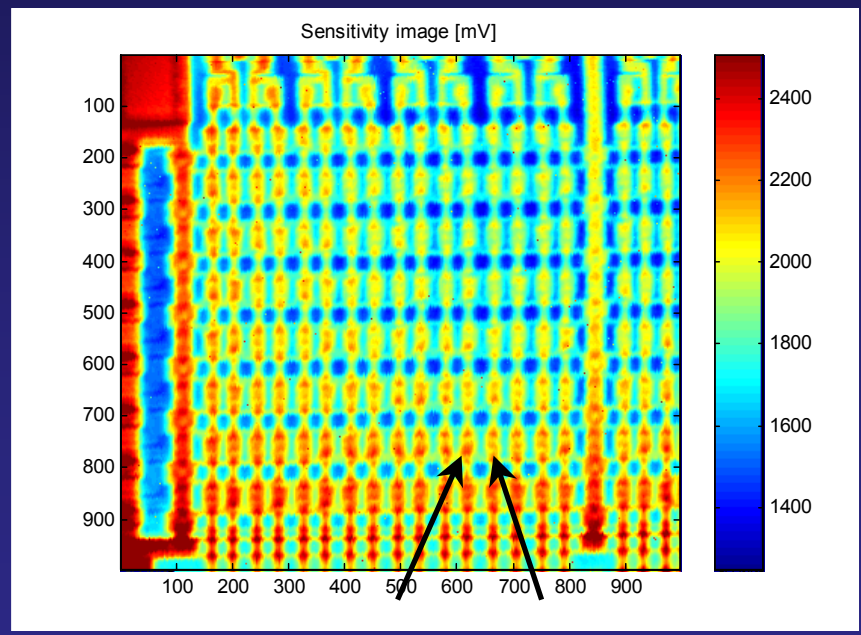
Motorola MC68HC705P6A microcontroller

Semi-invasive imaging techniques

Advanced imaging techniques – laser scanning

- Mask ROM extraction without chemical etching
  - Also works from the rear side of a chip
  - Resolution is limited by wavelength of the infrared laser, works down to 0.5 µm process





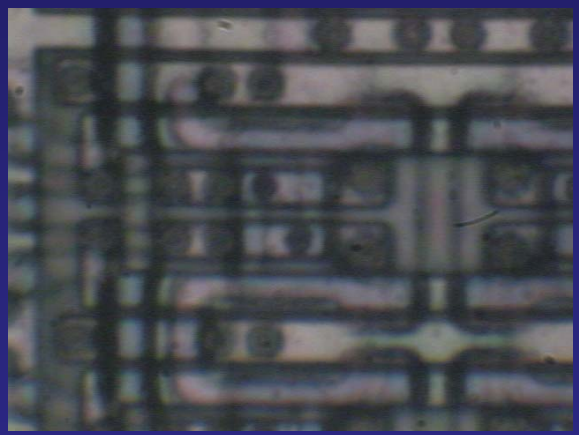
Motorola MC68HC705P6A microcontroller

Further improvements to the OEPA

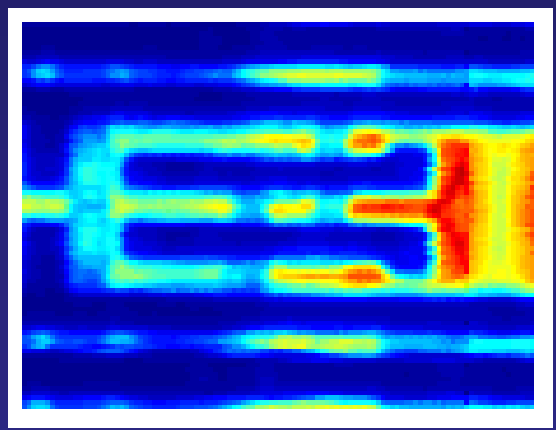
Modern chips benefit from multiple metal layers and polished insulation layers restricting optical access

→ Rear-side access to SRAM (through silicon substrate)

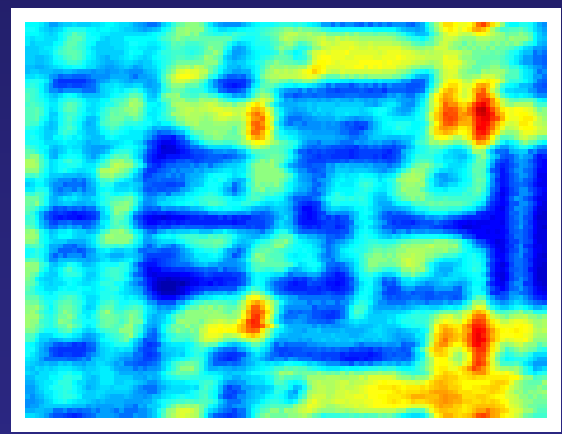
- Infrared lasers, optics and cameras must be used
- Thinning of the substrate is required for < 0.35 µm chips



PIC16F84 SRAM cell: optical image 100×



PIC16F84 SRAM cell: OBIC front image

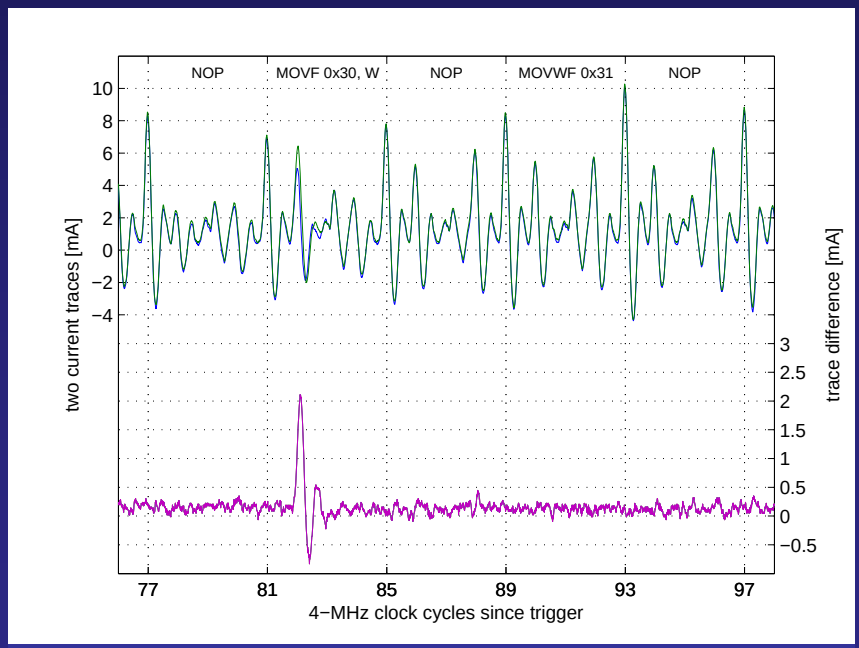


PIC16F84 SRAM cell: OBIC rear image

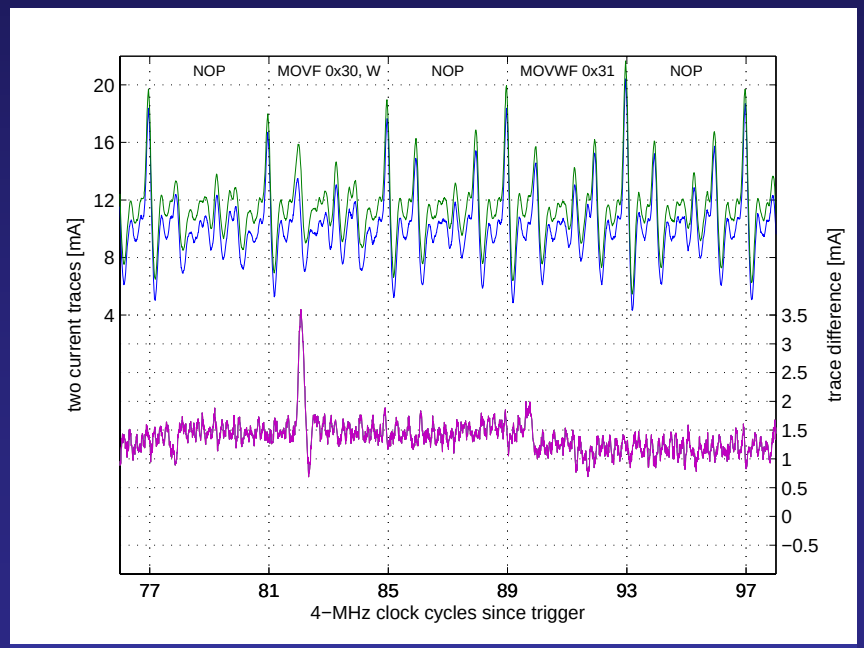
Results for the rear-side experiments

Laser focused on VT1+VT4 (n-channels) of memory cell

- State of the cell stays unchanged for low laser power
  - Response is very similar to the front side approach, but shifted due to spatial ionization of the bulk silicon substrate
  - Both read and write operations can be detected
- State changes for higher laser power



PIC16F84 front side, Read: (0xFF) − $(0xFF)_L$ (Av=1)



PIC16F84 rear side, Read: (0xFF) − $(0xFF)_L$ (Av=1)

Semi-invasive attacks vs other attacks

Comparing with invasive attacks

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

Comparing with non-invasive attacks

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

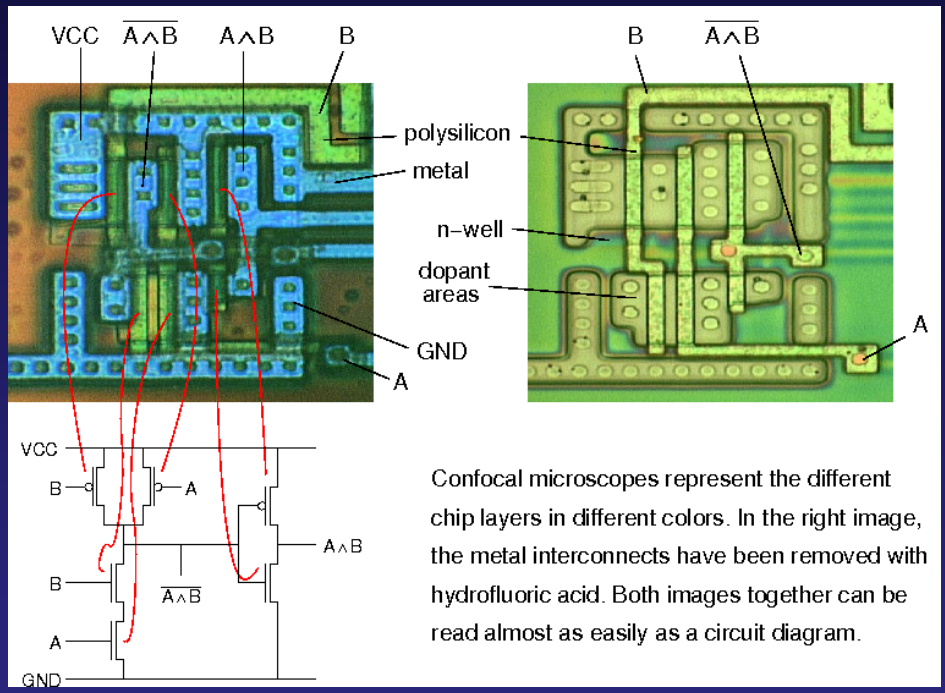
Equipment for semi-invasive research

Semi-invasive analysis using equipment from Semiconductors Research Ltd.

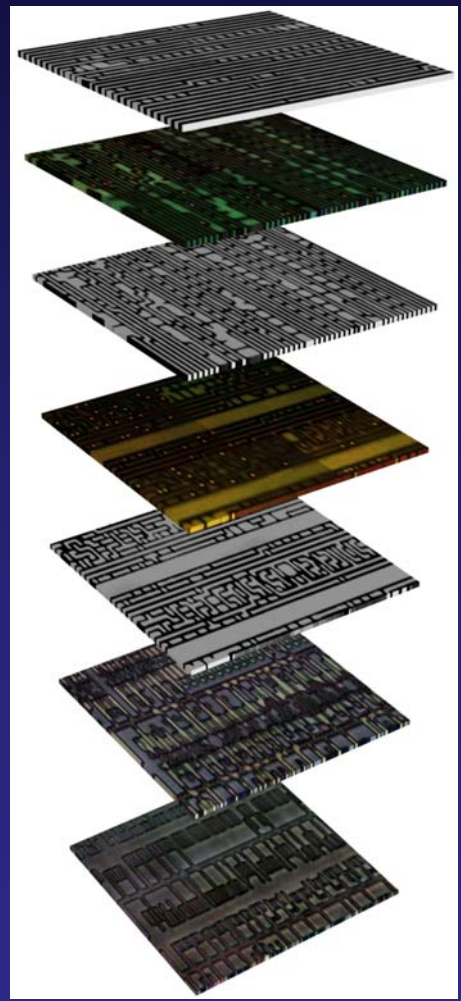
- Ex-demo version of Trioscan with NWR QuikLaze-II TriLaze laser cutter
  - Dual-mode advanced laser scanning
    - Large-area scanning (12×12 mm^2)
    - High-resolution scanning (0.05 µm)
  - Long-working distance objectives (10 mm minimum for high-magnification objectives)
  - Dual-use laser cutting system
    - Sample preparation
    - Fault injection (Trig in/out synchronisation)
  - Optical fault injection capability for NWR and BSL lasers (external triggering)
    - Evaluation showed that NWR pulsed laser is not suitable for some types of optical fault injection attacks
- Testing proved specially designed equipment is better for testing and evaluation

Applications for semi-invasive attacks

Partial reverse engineering (understanding functions of circuits)



Picture courtesy of Dr Markus Kuhn



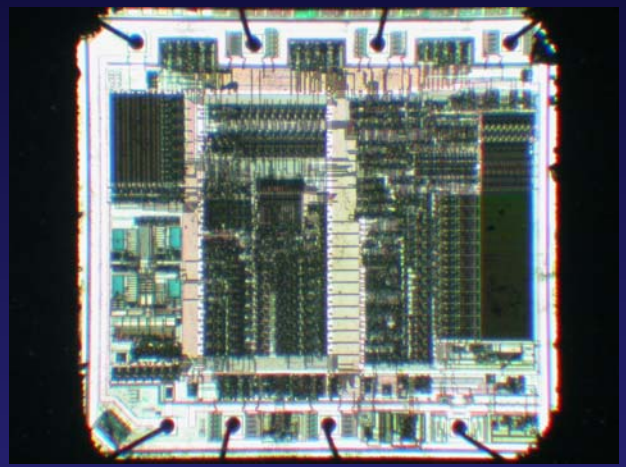
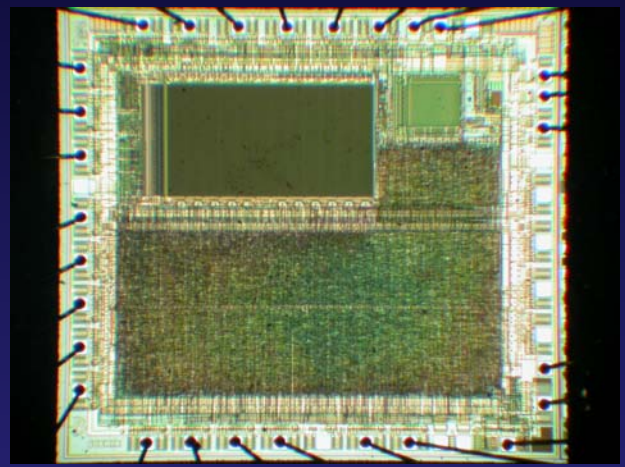
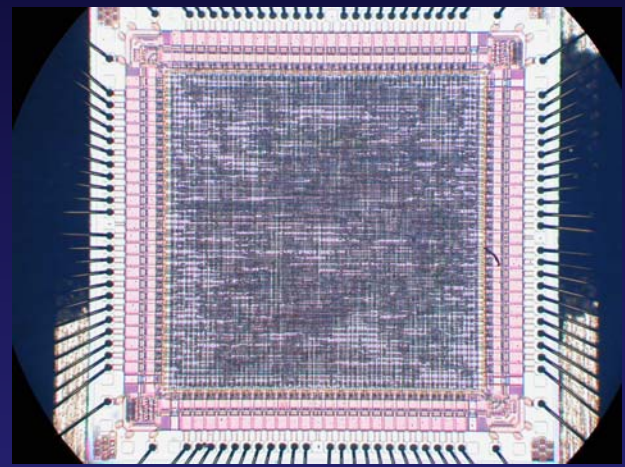
Picture courtesy of Semiresearch Ltd

Problems:

- feature sizes <0.2 µm
- number of transistors >1 million

Applications for semi-invasive attacks

- Time-critical and low-budget hardware security evaluation

- Non-penetrative hardware analysis
- Mass-production testing
- Forensic science

Further work

All results were achieved with a PIC16F84 microcontroller (~1 µm)

Modern microcontrollers are built with 0.18 µm…0.35 µm

Further improvements to rear-side access are required

- Substrate thinning and polishing
- Using high-end infrared lasers
  - better output power control
  - low-noise operation

We collaborate with industrial companies

- Designing new equipment for semi-invasive analysis techniques
- Developing new attack techniques and analysis methods

Conclusions

There are many ways a given system can be attacked and it is always possible to break the system with invasive attacks

Not all invasive attacks are very difficult and expensive to implement, but if there is a way to use semi-invasive attacks, it is always faster and cheaper

Semi-invasive attacks are less destructive to the device

Combination of different attack methods together could bring much better techniques

Semi-invasive analysis methods proved their effectiveness in hardware security evaluation against various attacks

Technical progress helps both defenders and attackers

Developing adequate protection, always estimate attacker's experience, knowledge and available tools