Optically Enhanced Position-Locked Power Analysis

Sergei Skorobogatov

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

A new attack technique

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

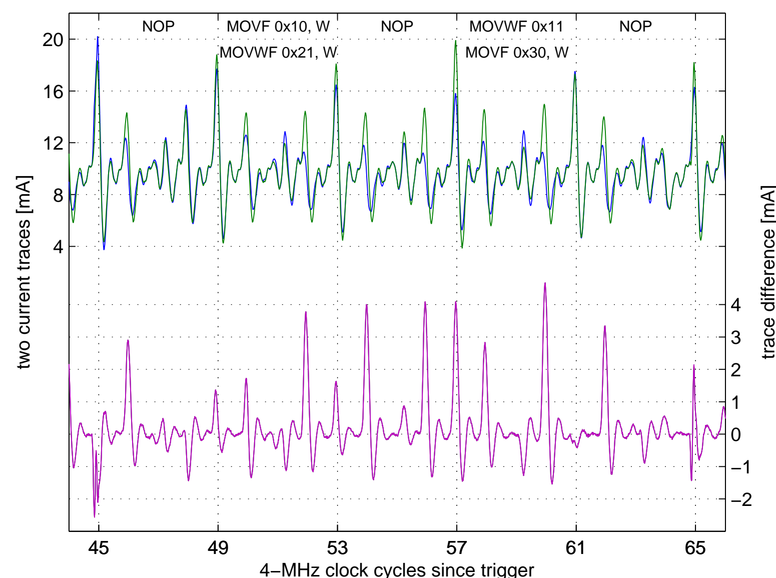
Reasons for developing the new attack technique

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

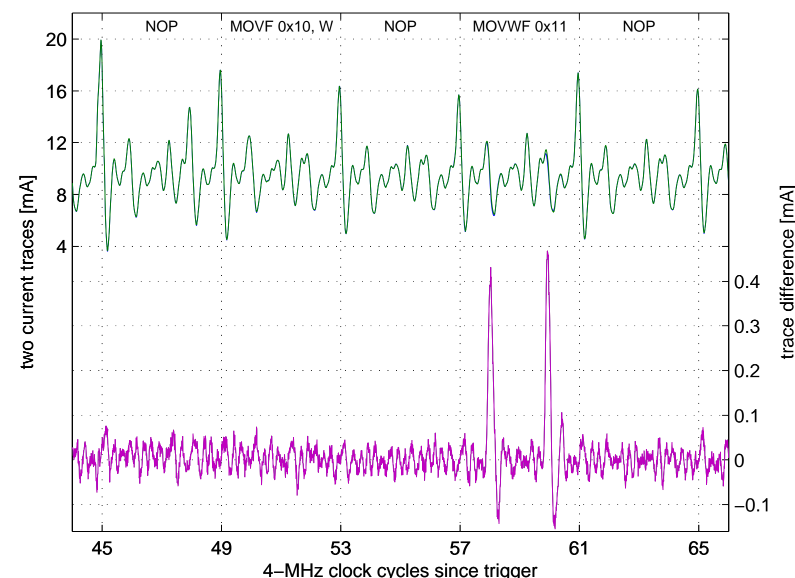
Conventional power analysis

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

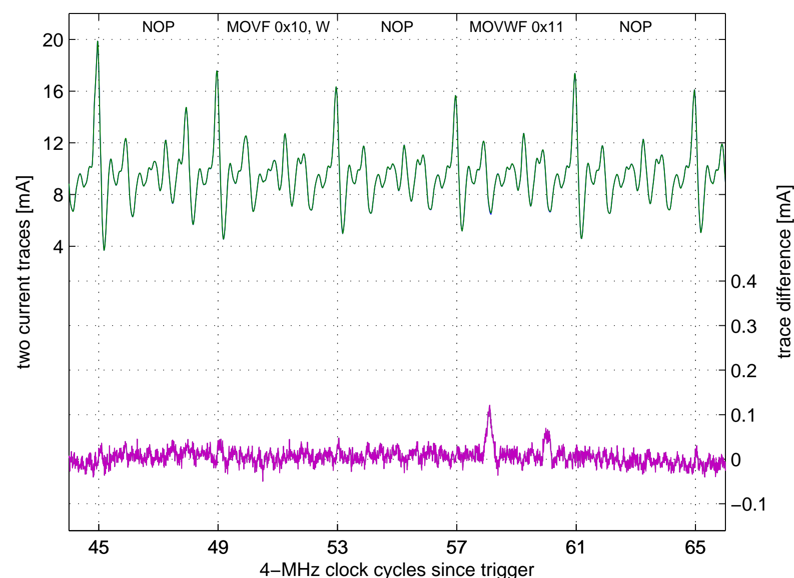


PIC16F84, Write: (0x00 → 0x00) − (0x01 → 0x00) (Av = 64)

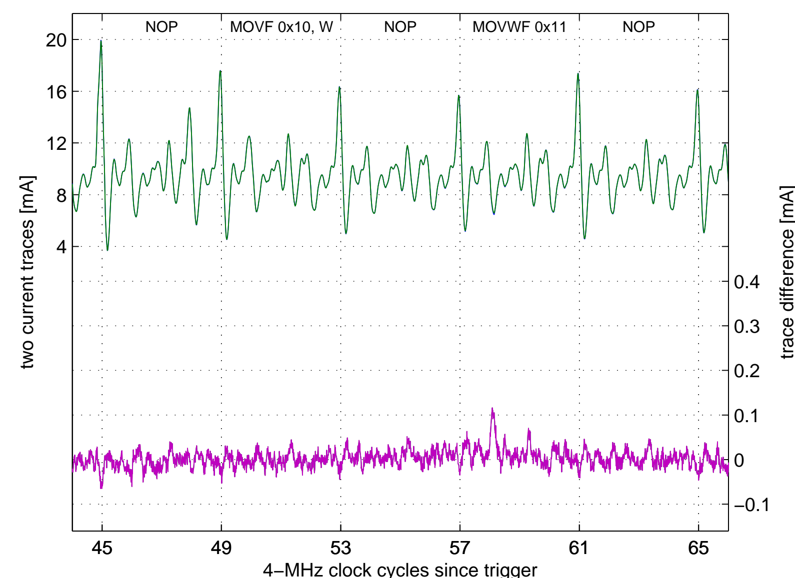
Conventional power analysis

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



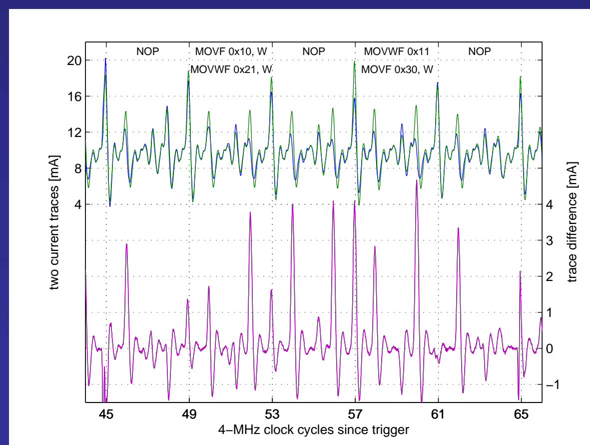
PIC16F84, Write: (0x01 → 0x00) − (0x10 → 0x00) (Av = 256)



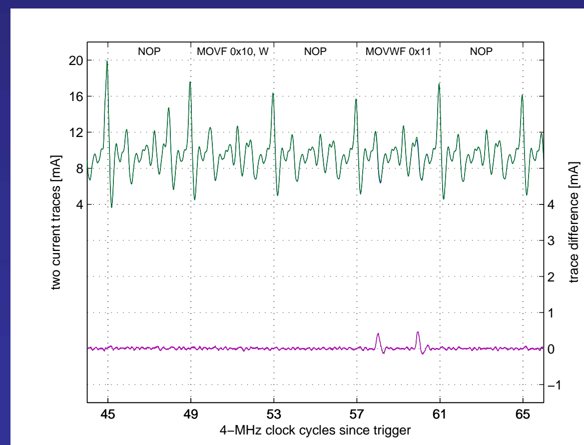
PIC16F84, Write: (0xF7 → 0x00) − (0xDF → 0x00) (Av = 256)

Power analysis summary

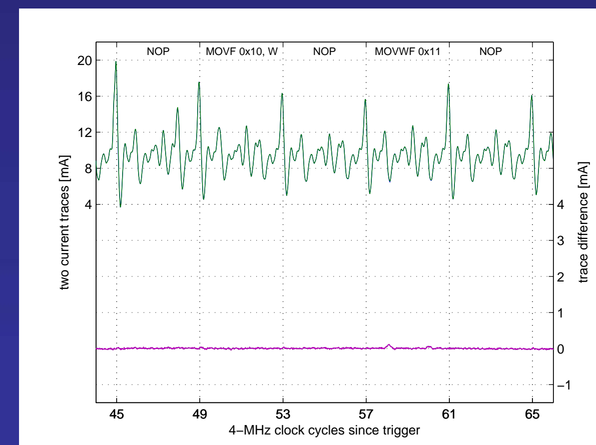
- Non-invasive attack with a simple setup
- Measurements applied for a whole chip rather than on a small area
- Averaging is essential to distinguish between small changes in data values, hence longer measurement time
- Detects only changes in data values rather than their absolute value
- Data dependency 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)

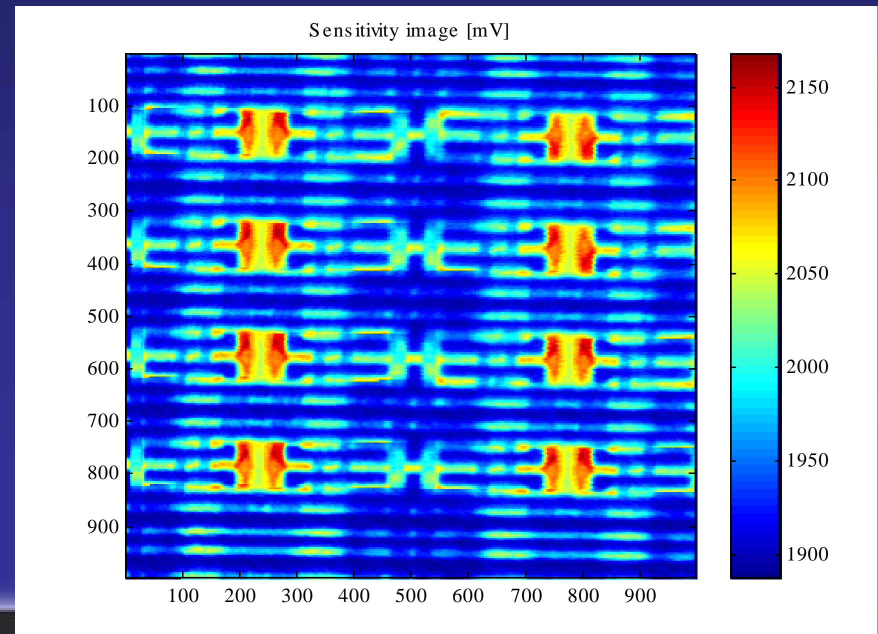


Write: (0x01→0x00) − (0x10→0x00) (Av = 256)

Semi-invasive methods

Use lasers to probe device operation

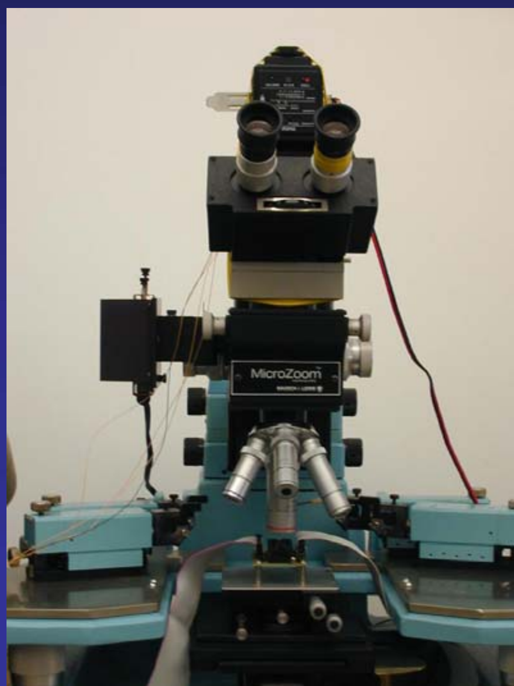
- Require access to the chip surface without mechanical contact
- Widely used in failure analysis of semiconductors (LIVA, TIVA)
  - Determine state of CMOS transistors in static mode
- Direct observation of signals inside a semiconductor (polarization)
  - Expensive setup and special sample preparation
- 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

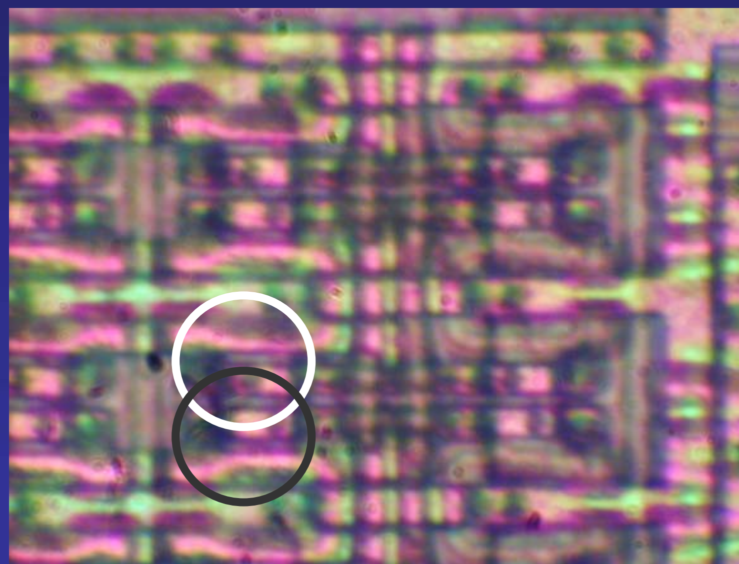


Semi-invasive methods

Use lasers to interfere with device operation

- Optical fault injection attacks
  - Relatively inexpensive setup (photoflash & microscope)
  - Scalable down to a single inverter in SRAM cell
  - Memory cell changes its state (→ detectable by software)





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) and non-invasive (power analysis) methods to reliably detect a single bit change without interfering with normal device operation?

Can we avoid averaging?

Can we increase the response?

Countermeasures?

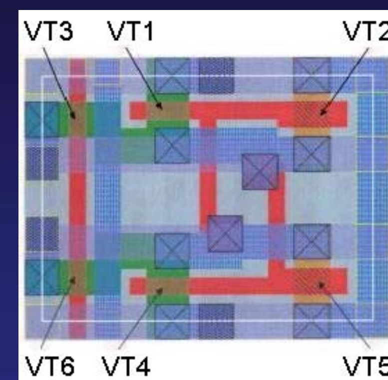
Why an SRAM cell?

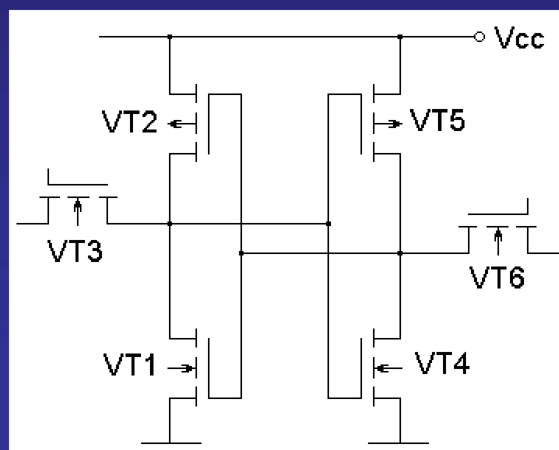
Widely used in modern devices as volatile memory

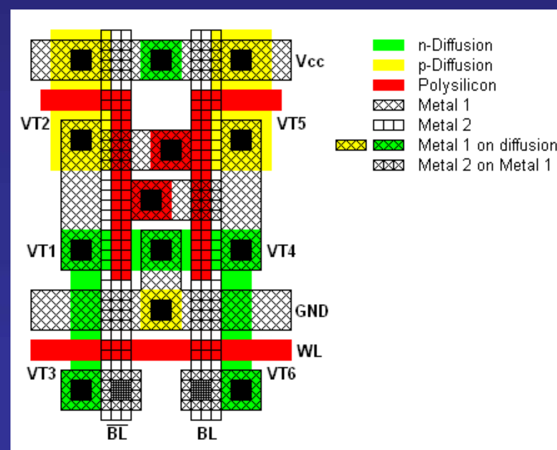
- CPU registers, Data memory, Cache memory

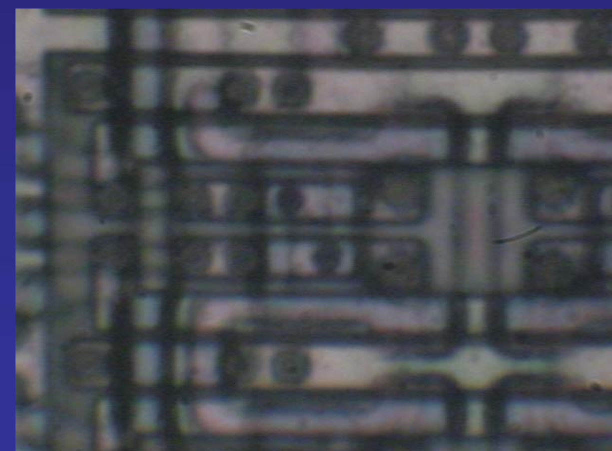
As a result, all cryptographic algorithms and password authentication go through it

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





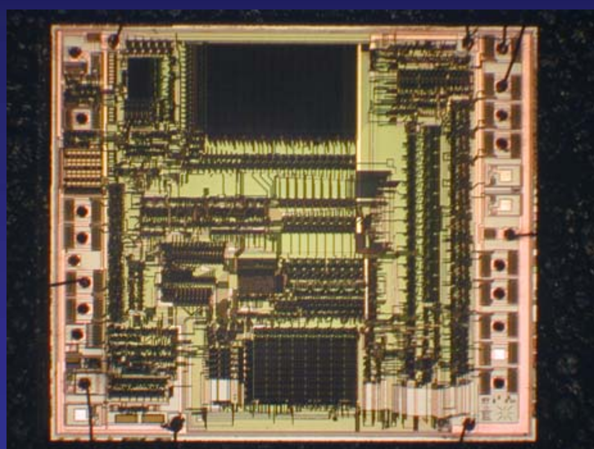


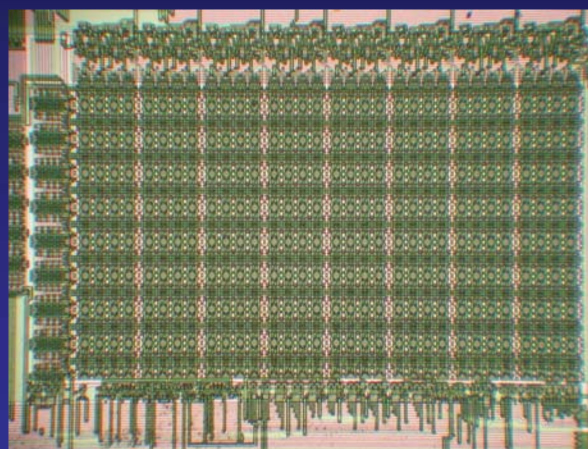


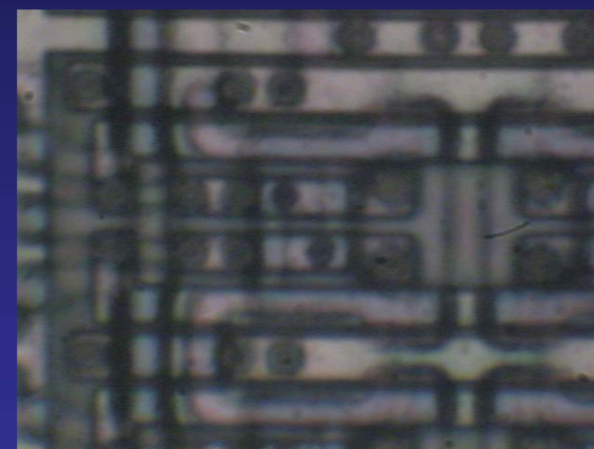
Experimental setup

Target of evaluation: PIC16F84 microcontroller

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







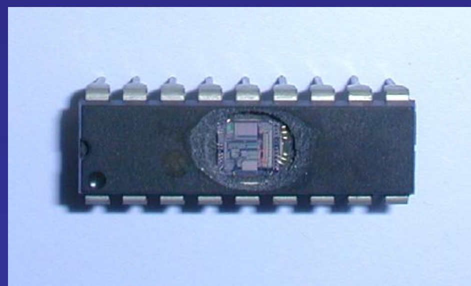
bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0

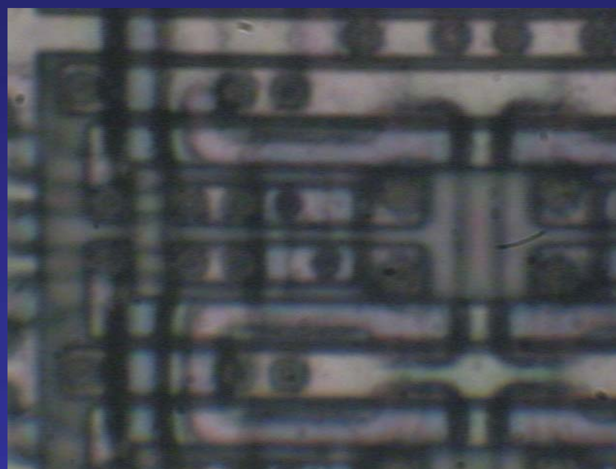
30h	34h	38h	3Ch	40h	44h	48h	4Ch	10h	14h	18h	1Ch	20h	24h	28h	2Ch	0Ch
31h	35h	39h	3Dh	41h	45h	49h	4Dh	11h	15h	19h	1Dh	21h	25h	29h	2Dh	0Dh
32h	36h	3Ah	3Eh	42h	46h	4Ah	4Eh	12h	16h	1Ah	1Eh	22h	26h	2Ah	2Eh	0Eh
33h	37h	3Bh	3Fh	43h	47h	4Bh	4Fh	13h	17h	1Bh	1Fh	23h	27h	2Bh	2Fh	0Fh

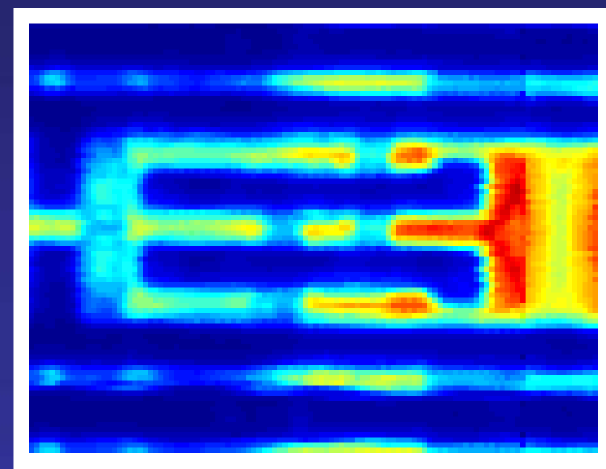
Experimental setup

PIC16F84: Finding active locations

- Decapsulated samples prepared in a standard way
- Light-sensitive locations found using OBIC laser-scan technique





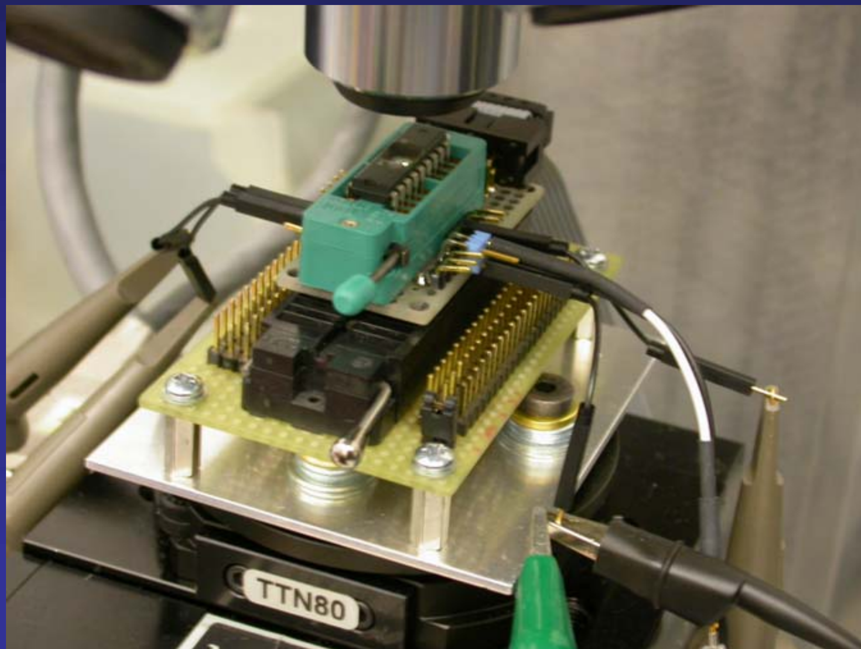


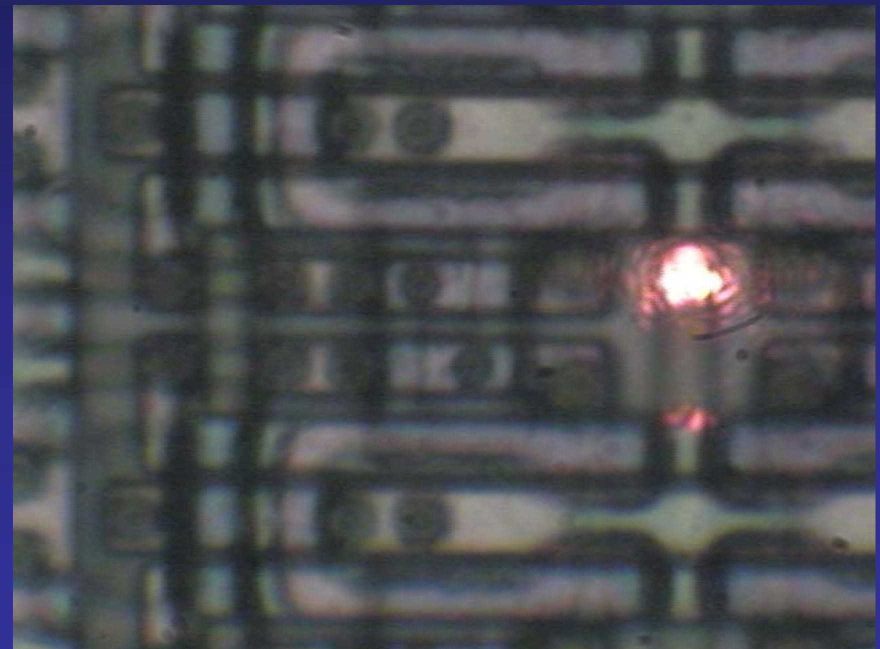
Experimental setup

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

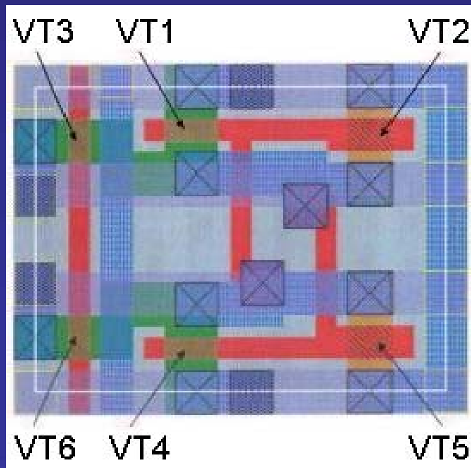


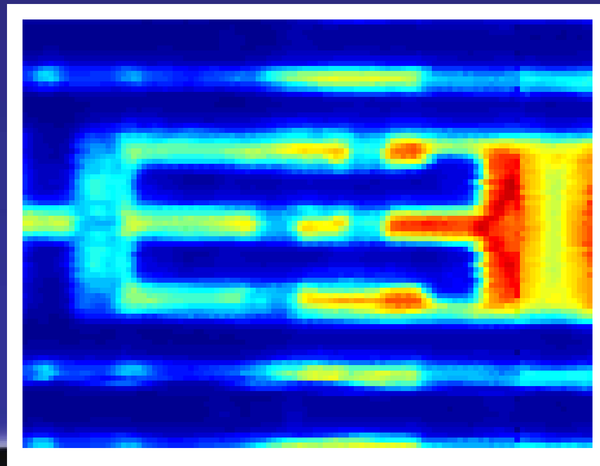


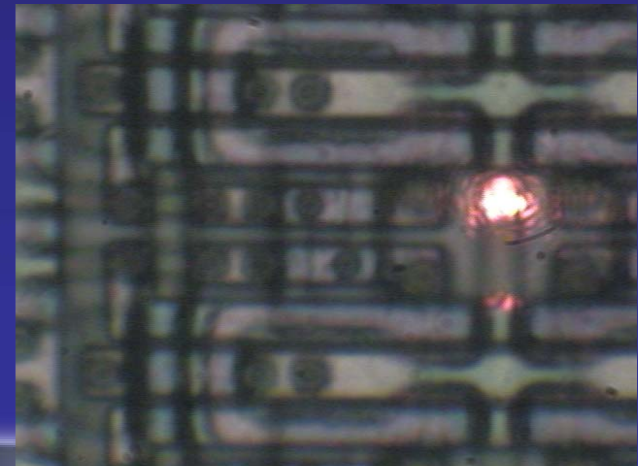
Experimental setup

PIC16F84: Test sequence

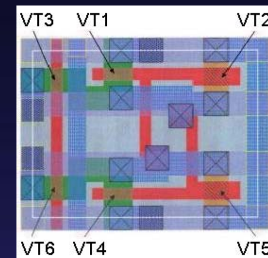
- Microcontroller programmed with a test code
  - Generate trigger pulse for oscilloscope
  - Read from the SRAM memory locations
  - Write to the SRAM memory locations
  - Dump SRAM memory for verification
- Known physical location and layout for all SRAM cells
- Light-sensitive locations for VT1…VT6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





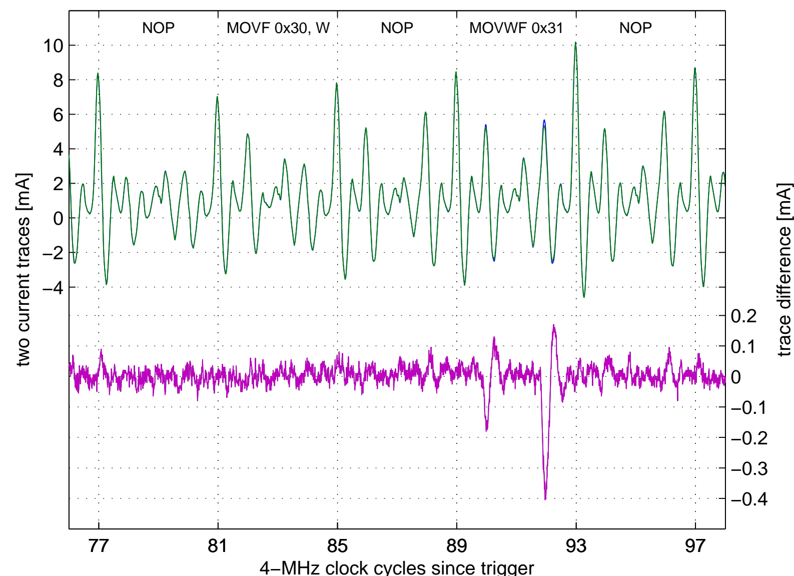


Results

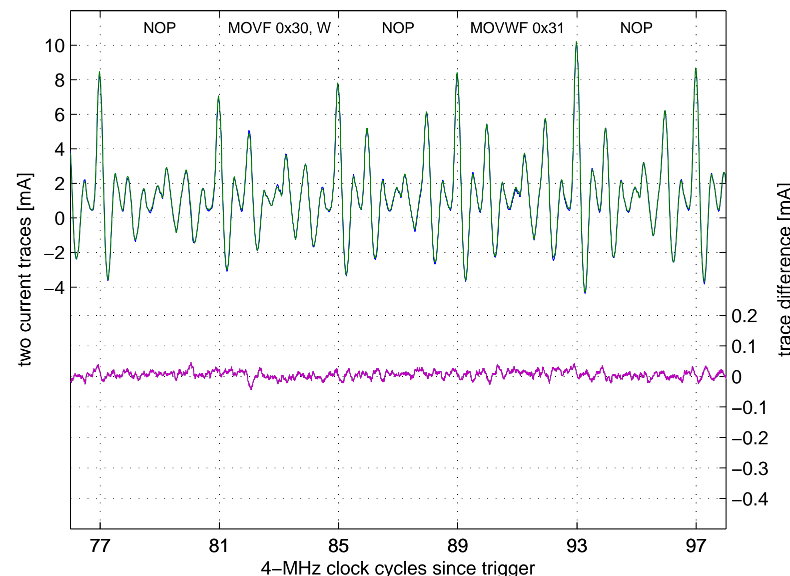


Laser focused on VT1 (n-channel) of the SRAM cell

- 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



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

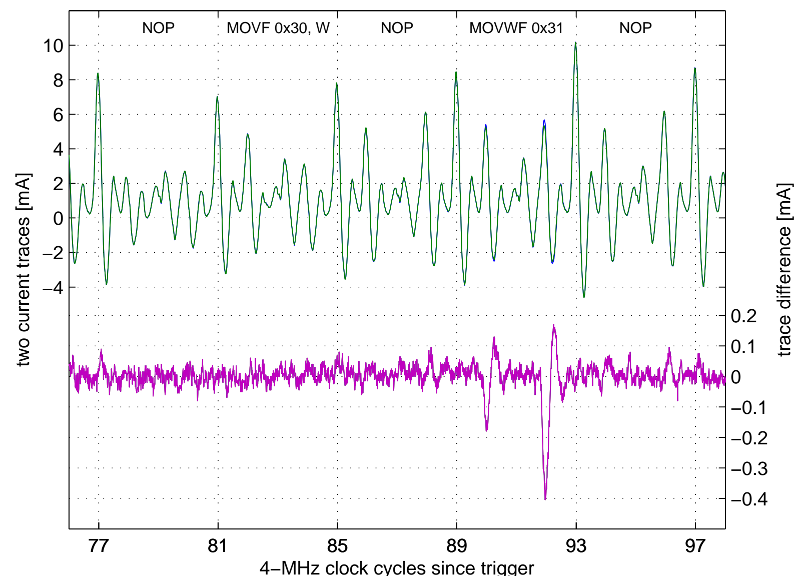


PIC16F84, Read: (0xFF) − $(0xFF)_L$ (Av = 256)

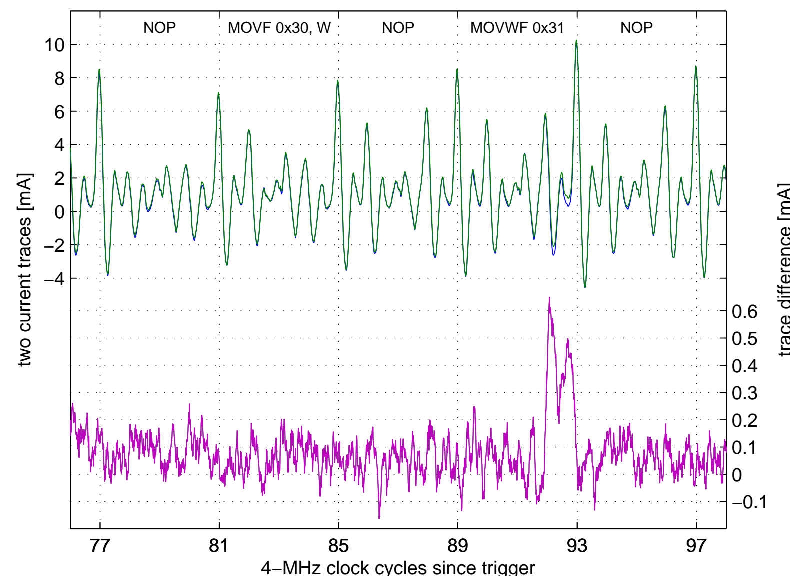
Results

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)

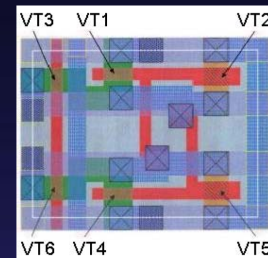


PIC16F84, Write: (0x00 → 0xFF) − $(0x00 \rightarrow 0xFF)_L$ (Av = 16)



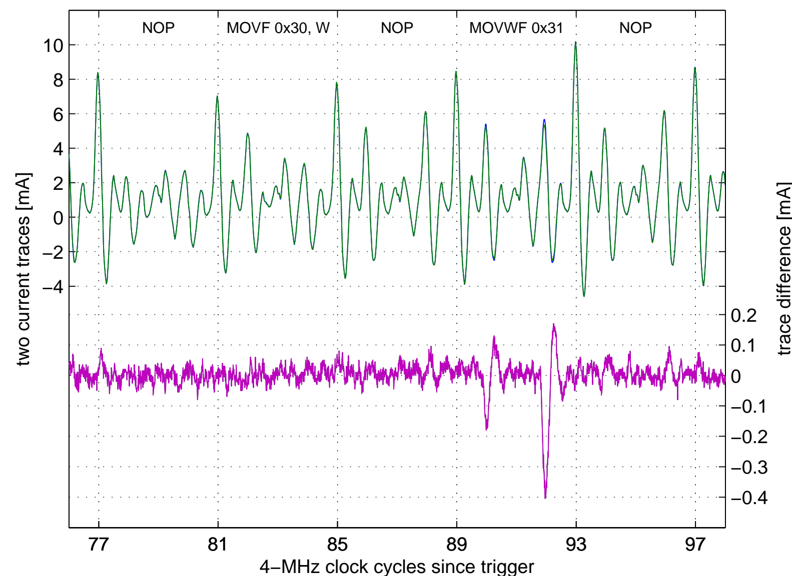
PIC16F84, Write: (0x00 → 0xFF) − $(0x00 \rightarrow 0x7F)_L$ (Av = 1)

Further improvements to the results

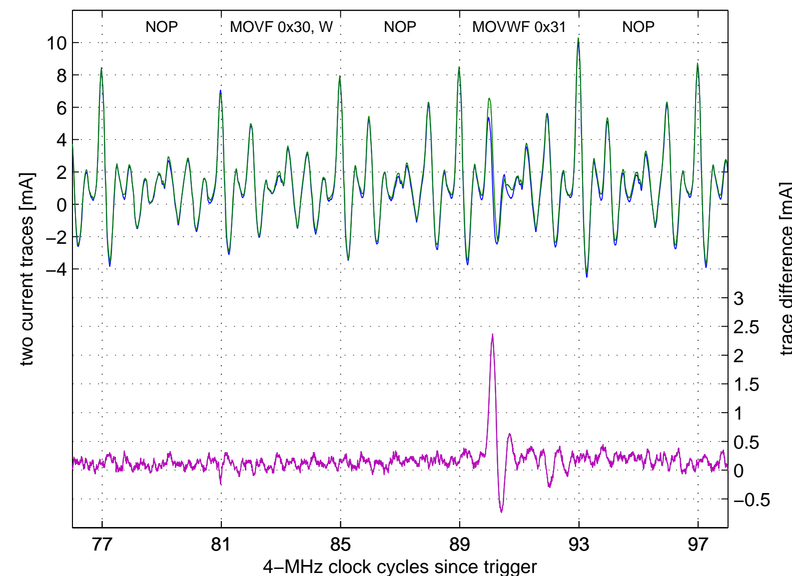


Laser focused on VT1+VT4 of the SRAM cell

- 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 → 0xFF)$_L$ (Av = 16)

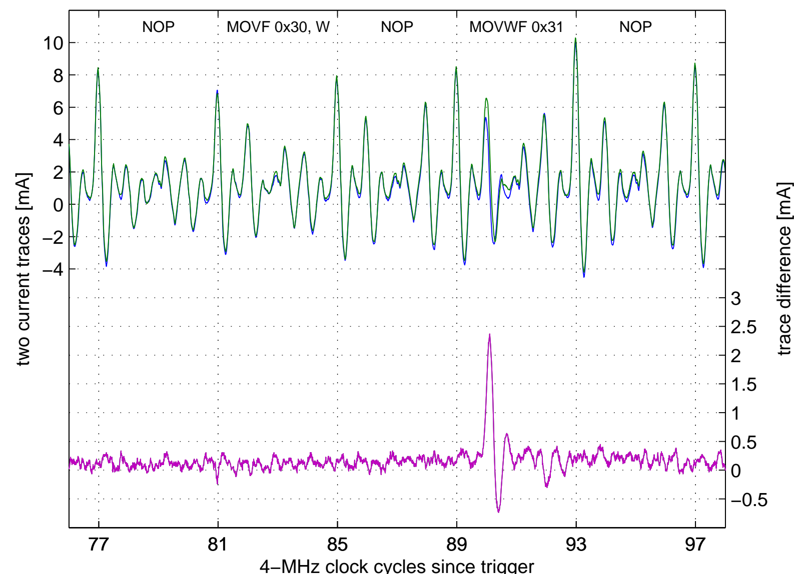


PIC16F84, Write: (0x00 → 0xFF) − (0x00 → 0xFF)$_L$ (Av = 1)

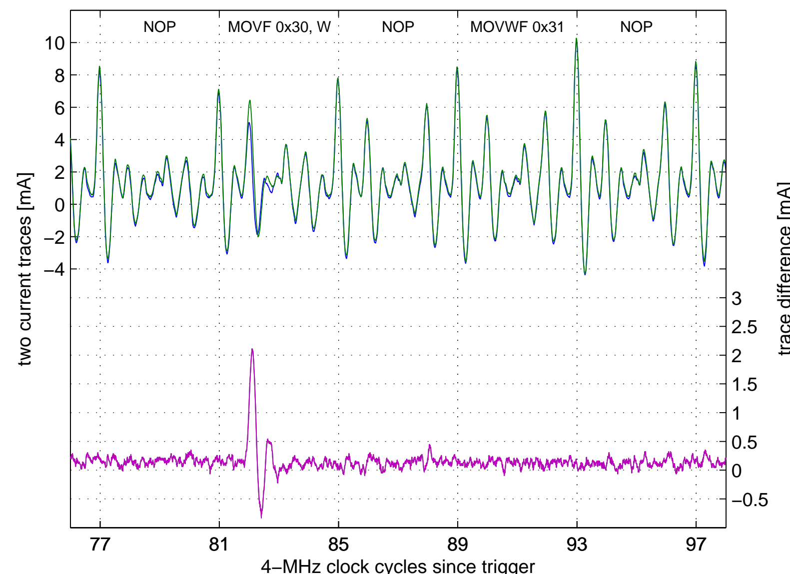
Results

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)

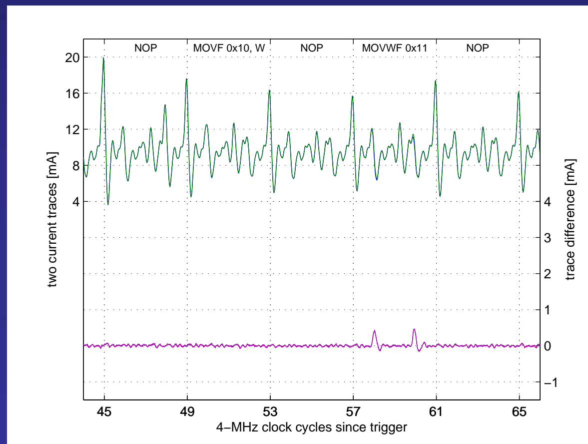


PIC16F84, Read: (0xFF) − (0xFF)$_L$ (Av = 1)

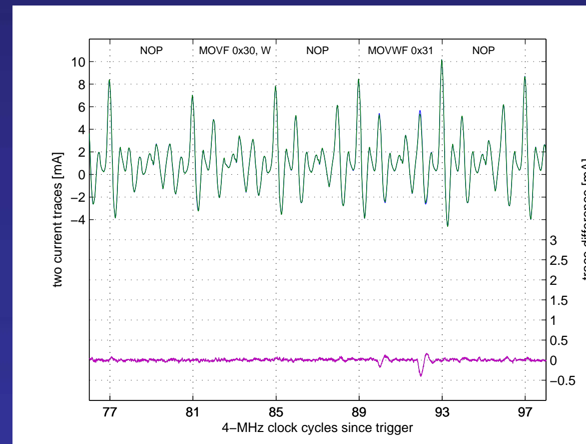
Explaining the results

Why this high response with the laser on VT1+VT4?

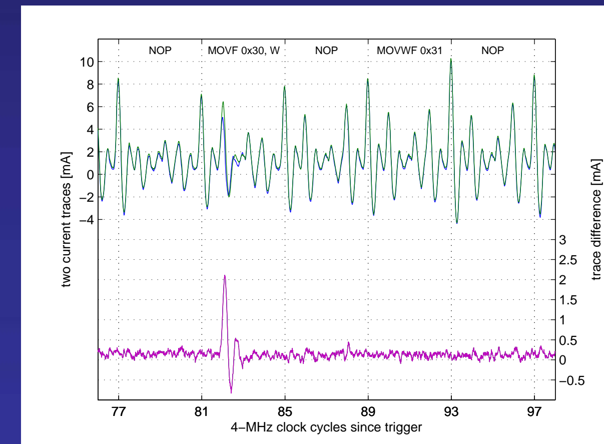
- Compared to single-bit difference in data: 5 times higher
- Compared to the laser on VT1 results: 6…10 times higher



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



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

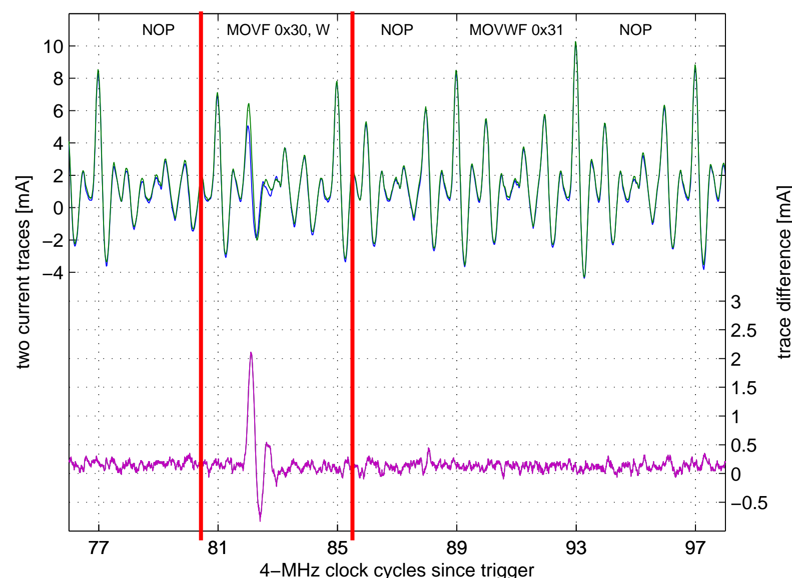


PIC16F84, Read: (0xFF) − $(0xFF)_L$ (Av = 1)

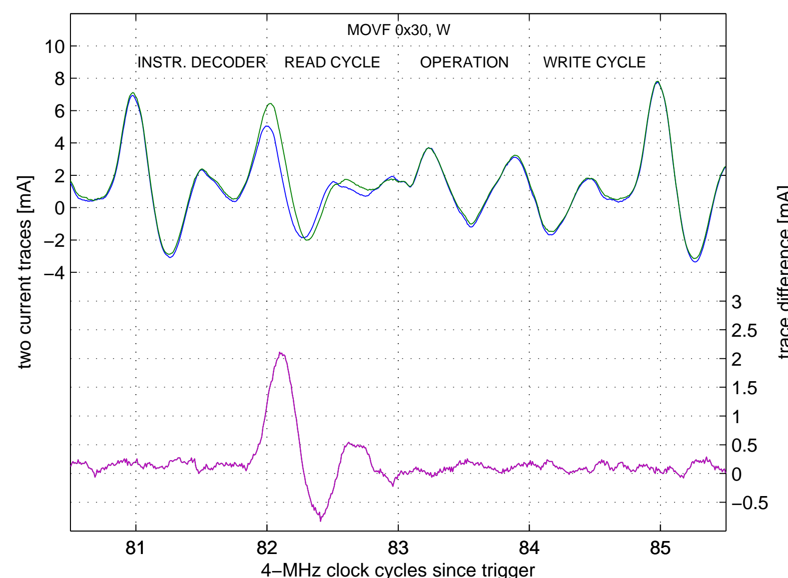
Explaining the results

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

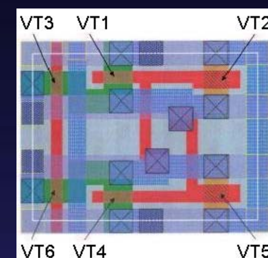


PIC16F84, Read: (0XFF) − $(0xFF)_L$ (Av = 1)



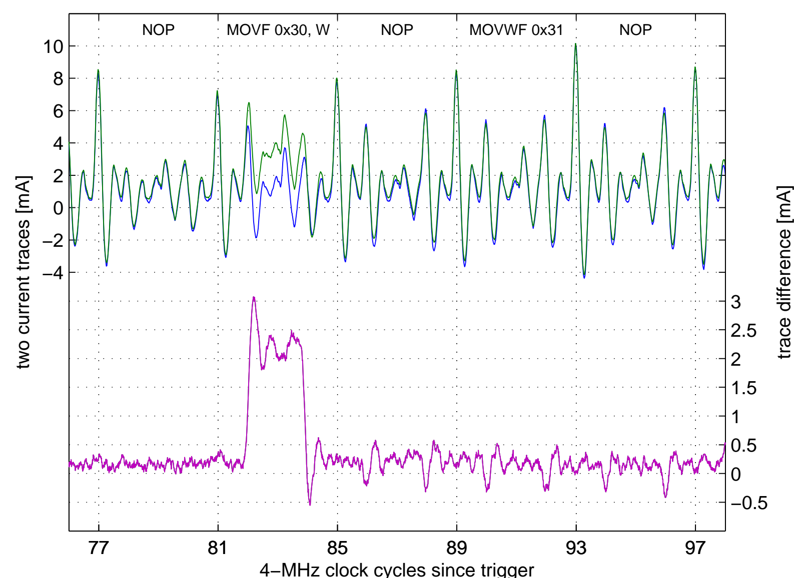
PIC16F84, Read: (0xFF) − $(0xFF)_L$ (Av = 1), ZOOM IN

Applications for higher laser power

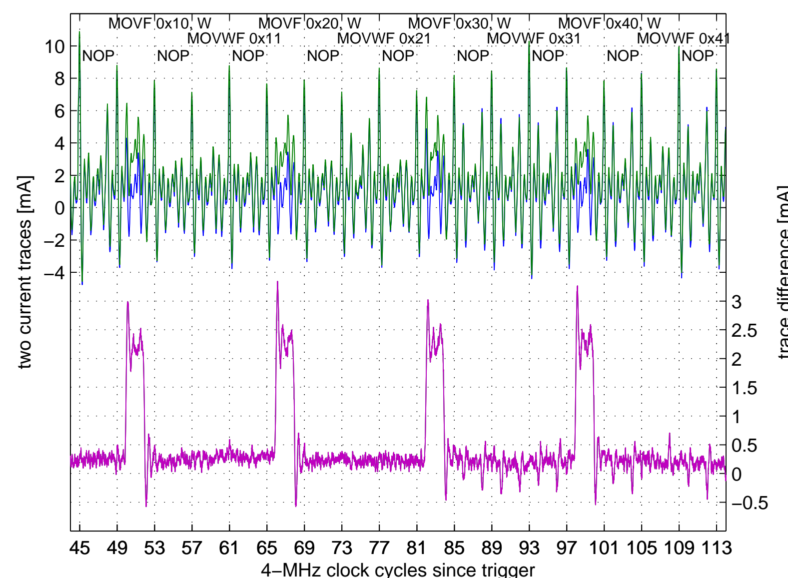


State of the memory cell is likely to change

- 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

For most applications averaging is not required

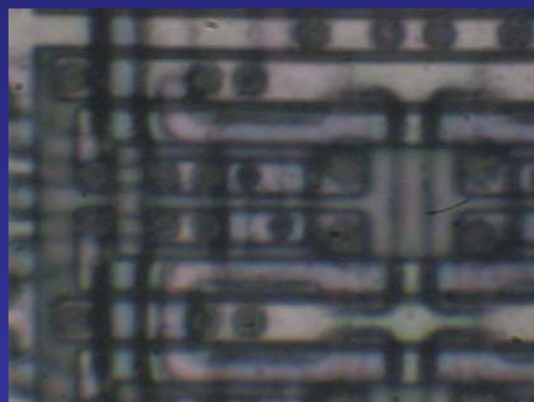
	SPA	LIVA	ΔOBIC	OEPA
State of SRAM cell	No	Yes	Yes	Yes
Access to SRAM cell	Limited	No	Limited	Yes
State change of SRAM cell	Yes	No	Limited	Yes
Real-time measurement	Yes	No	Limited	Yes

Further improvements to the method

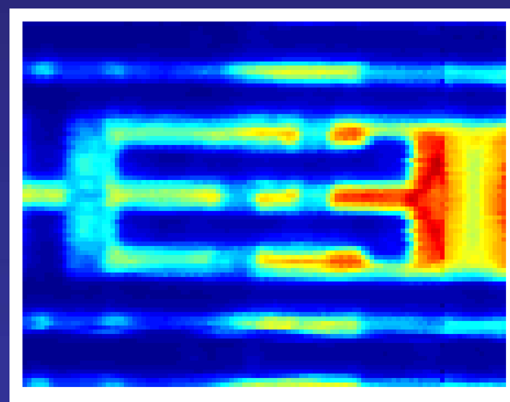
Modern chips benefit from multiple metal layers and polished insulation layers restricting optical access

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

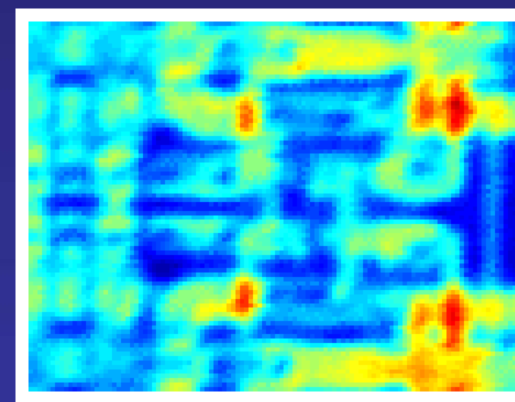
- Infrared lasers, optics and cameras must be used
- Thinning of the substrate is required for < 0.35 μm chips



PIC16F84 SRAM cell: optical image 100×



PIC16F84 SRAM cell: OBIC front image

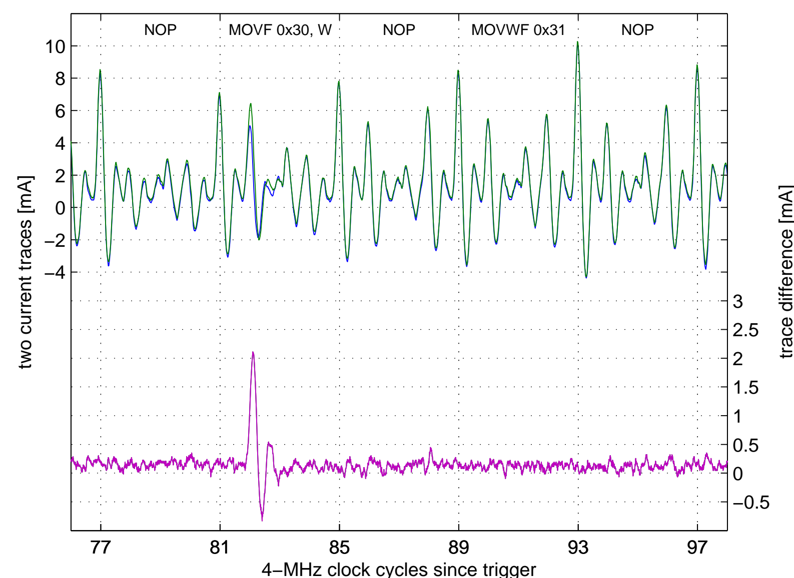


PIC16F84 SRAM cell: OBIC rear image

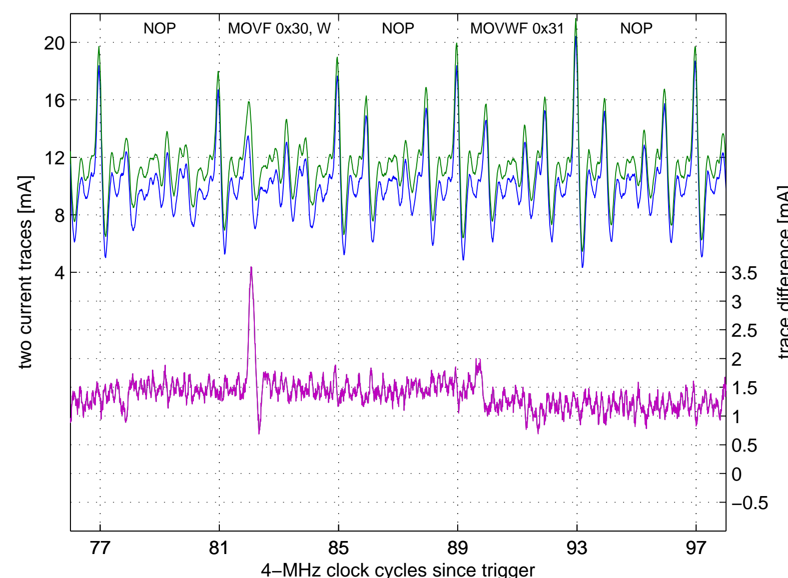
Results for the rear-side experiments

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)

Further work

These results were for a PIC16F84 microcontroller (~1 μm)

Modern microcontrollers are built with 0.18 μm…0.35 μm

Further improvements to rear-side access is required

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

Conclusions

1. It is possible to detect the internal state of memory cells using conventional optical probing methods
2. Optically enhanced power analysis (OEPA) significantly improves the results without interfering with the device operation
3. Compared to conventional power analysis, OEPA allows detection of individual bit changes
4. OEPA provides event detection capability

Countermeasures

- Modern technology (small feature size, multiple metal layers)
- Top metal protection, highly doped silicon and opaque cover
- Encrypted memory
- …