# Optically Enhanced Position-Locked Power Analysis

Sergei Skorobogatov

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

# A new attack technology

Combines

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

Application: Monitoring instructions and data

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

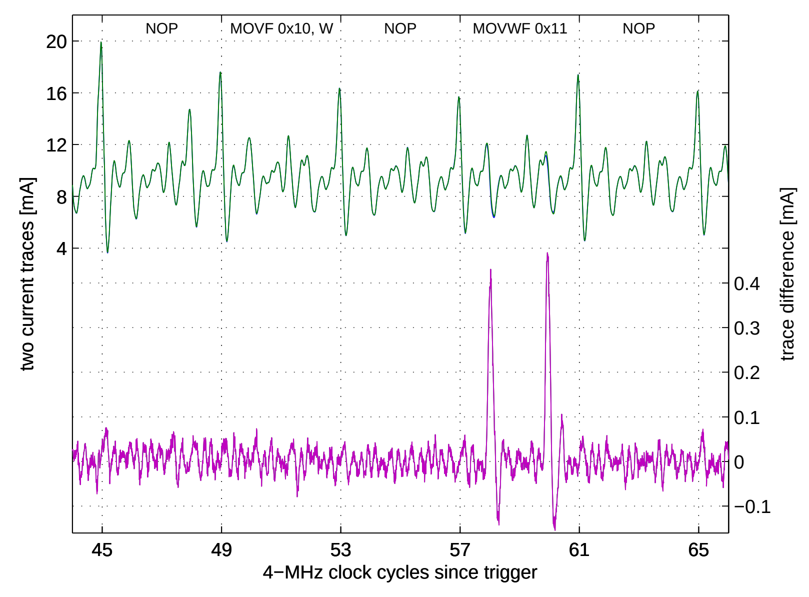
Advantages

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

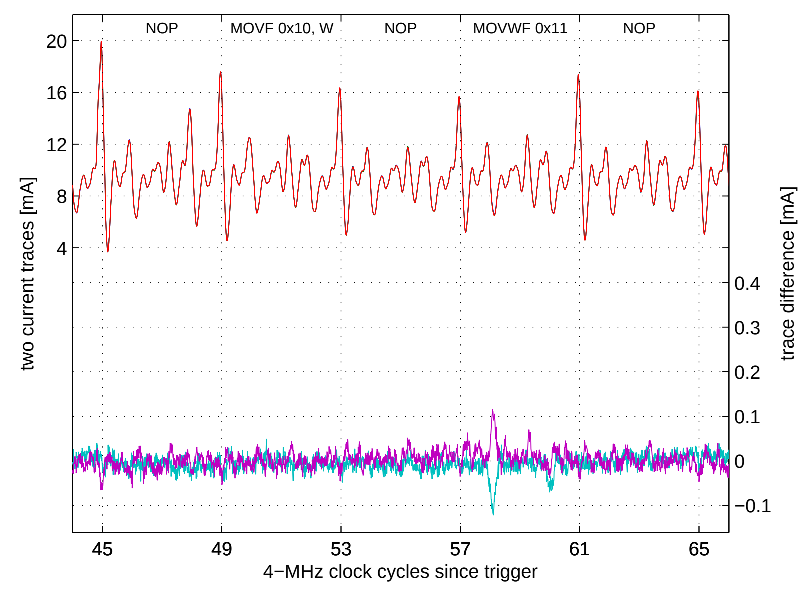
# Conventional power analysis

Measuring power consumption during device operation

- Non-invasive attack with simple setup
- Use averaging to reduce noise and increase resolution
- Very hard to distinguish values with the same Hamming weight
  - Sometimes possible if small number of bits has changed (01 vs 10; 0A vs 22)



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

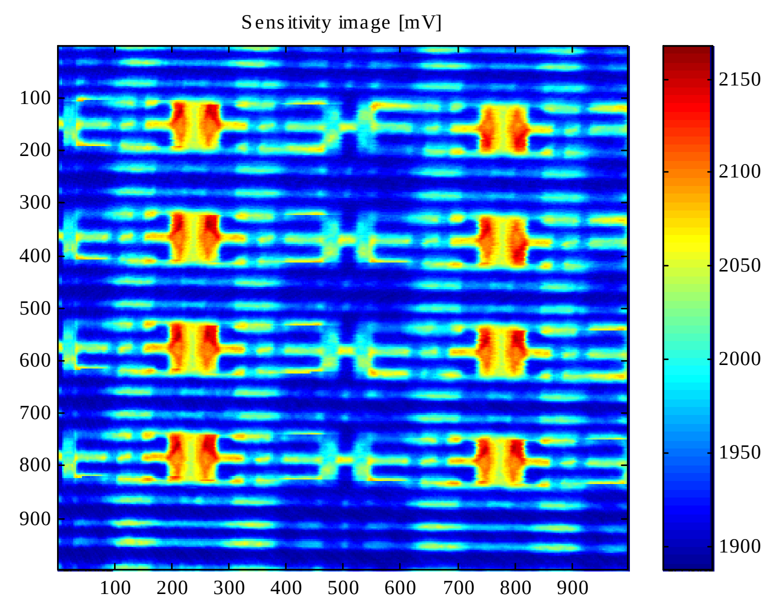


(0x01→0x00) − (0x10→0x00);  (0x0A→0x00) − (0x22→0x00)  (Av=256)

# Semi-invasive methods

Use lasers to probe device operation

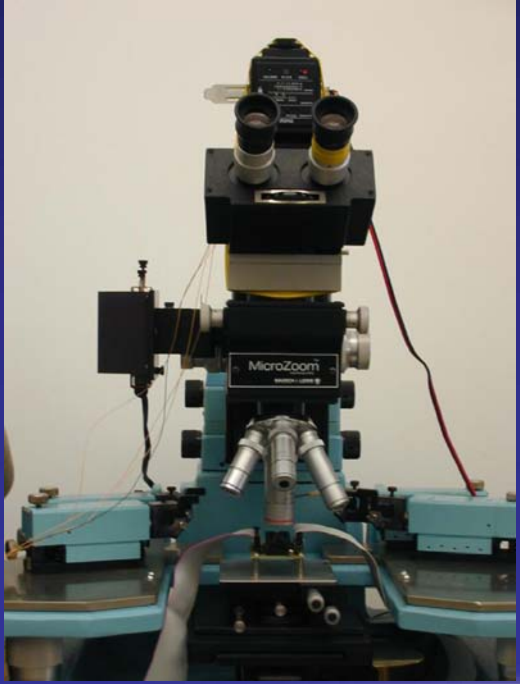
- Require access to the chip surface without mechanical contact
- Widely used in failure analysis of semiconductors (LIVA, TIVA)
  - Determine state of CMOS transistors in static mode
- Direct observation of signals inside a semiconductor (polarization)
  - Expensive setup and special sample preparation
- Modified OBIC (delta OBIC)
  - Measures difference in power consumption
  - Does not change SRAM
  - Relatively high cost and low sensitivity

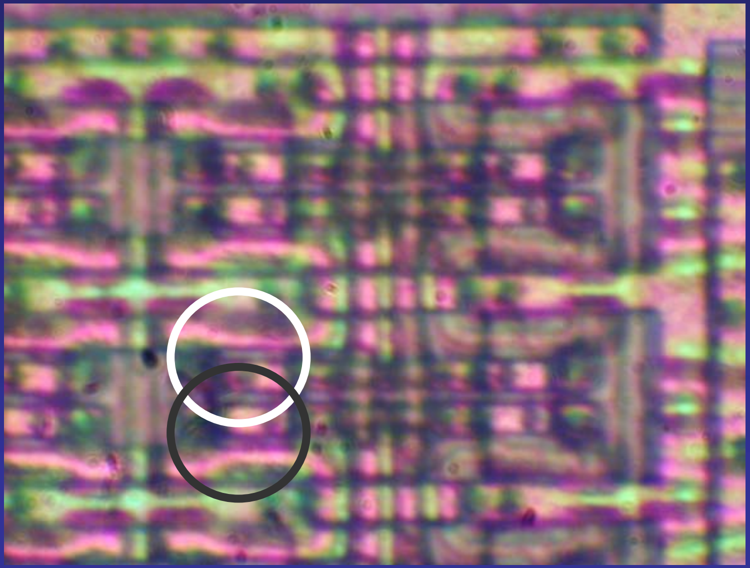


# Semi-invasive methods

Use lasers to interfere with device operation

- Optical fault injection (Skorobogatov, CHES 2002)
  - Relatively inexpensive setup
  - Scalable down to a single inverter in SRAM cell
  - Memory cell changes its state (→ detectable by software)





# 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?

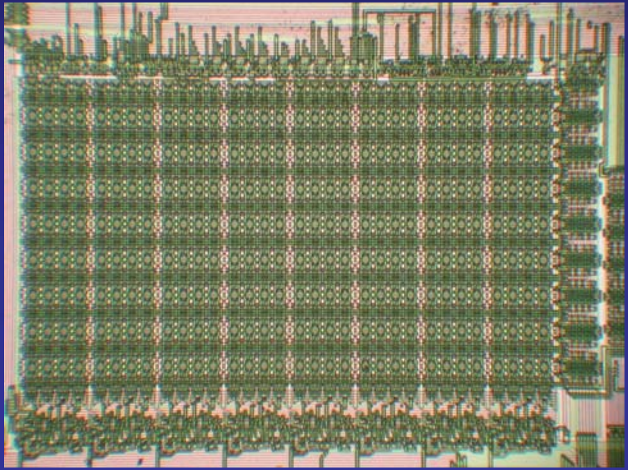
Can we increase the response?

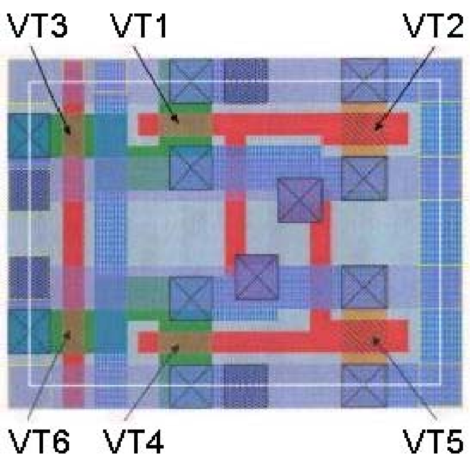
Countermeasures?

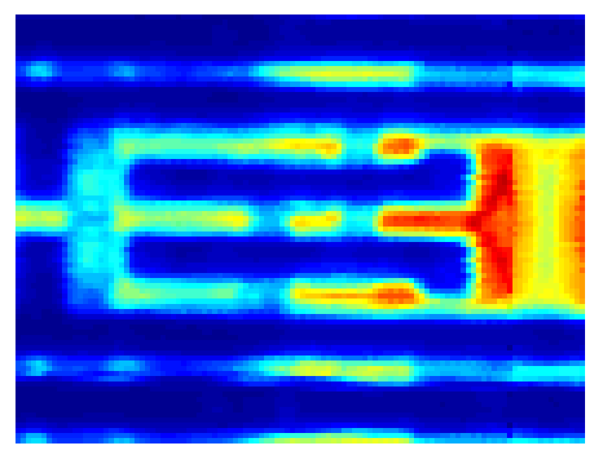
# Experimental setup

Target of evaluation: PIC16F84 microcontroller

- Decapsulated samples
- Known physical locations for all the SRAM cells (from optical fault injection experiments)
- Known layout of the SRAM cell
- Light-sensitive locations found using OBIC laser scan

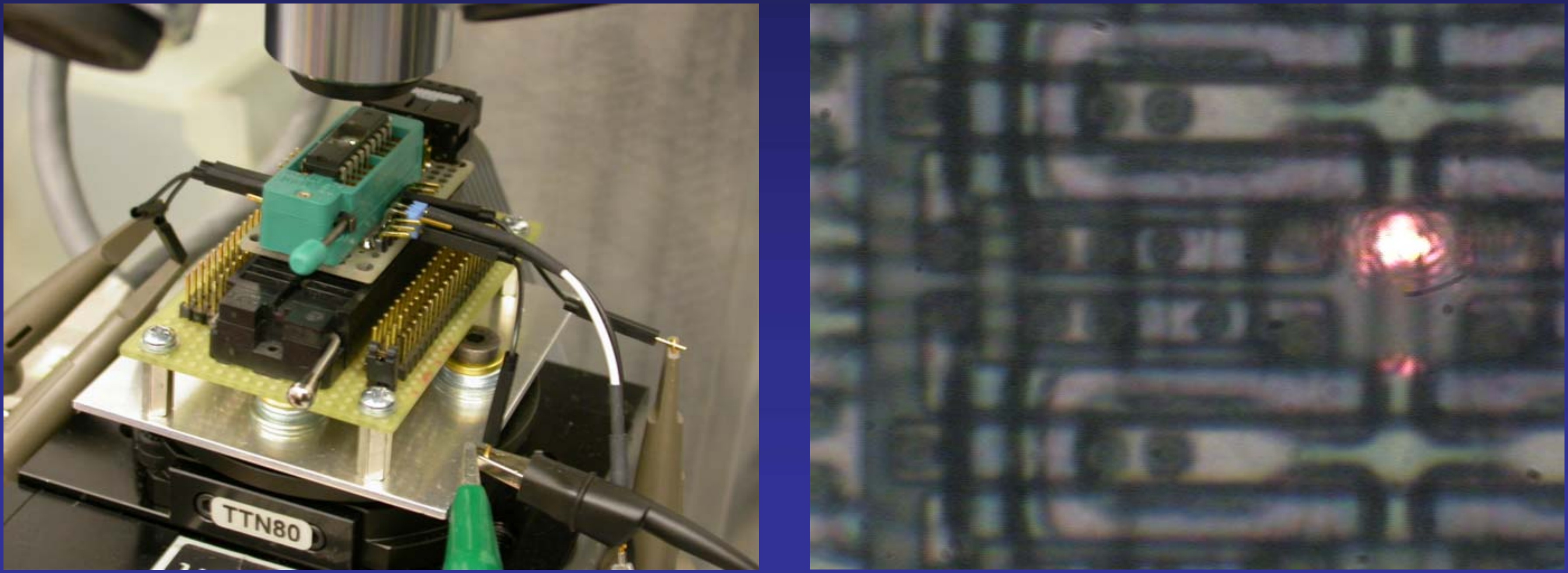






# Experimental setup

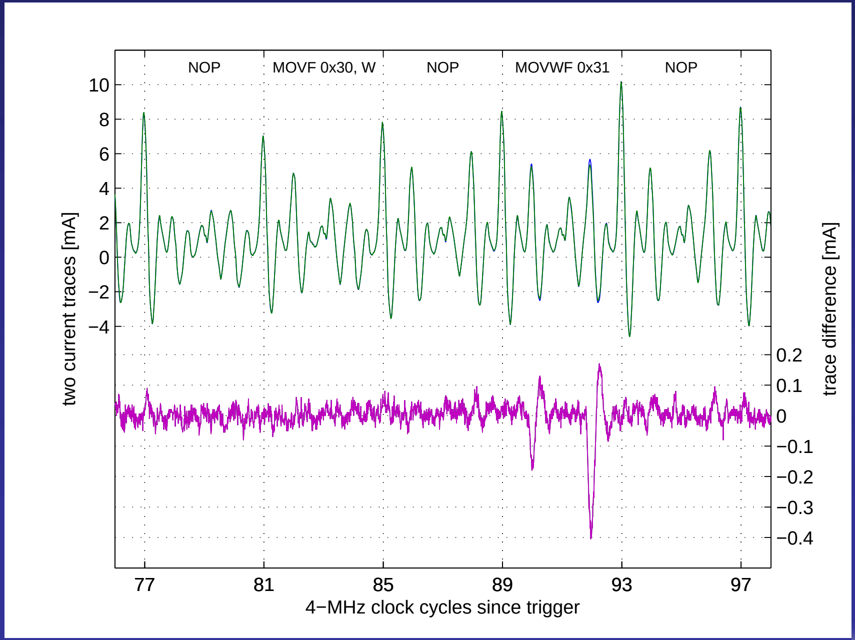
Decapsulated PIC16F84 on a test socket
Standard power analysis setup with 10 Ω in GND
Laser (639 nm, 1…3 mW) focused using 100× objective



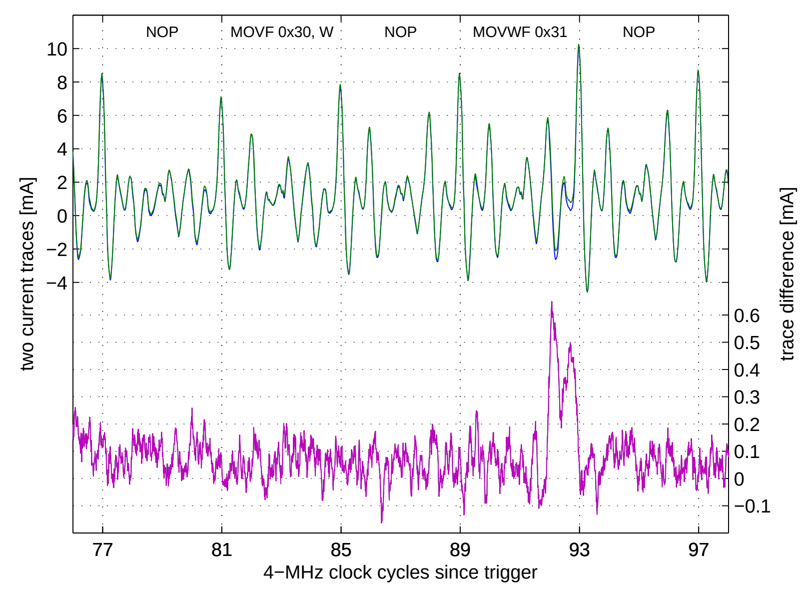
# Results

Laser focused on VT1 (n-channel) of memory cell 0x31

- State of the cell stays unchanged for low laser power
    - Maximum difference is less than power analysis result for a single bit change
    - Only write operations to the memory cell can be detected
- State of the cell changes for higher laser power
- The result is very similar to ΔOBIC or LIVA observation



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

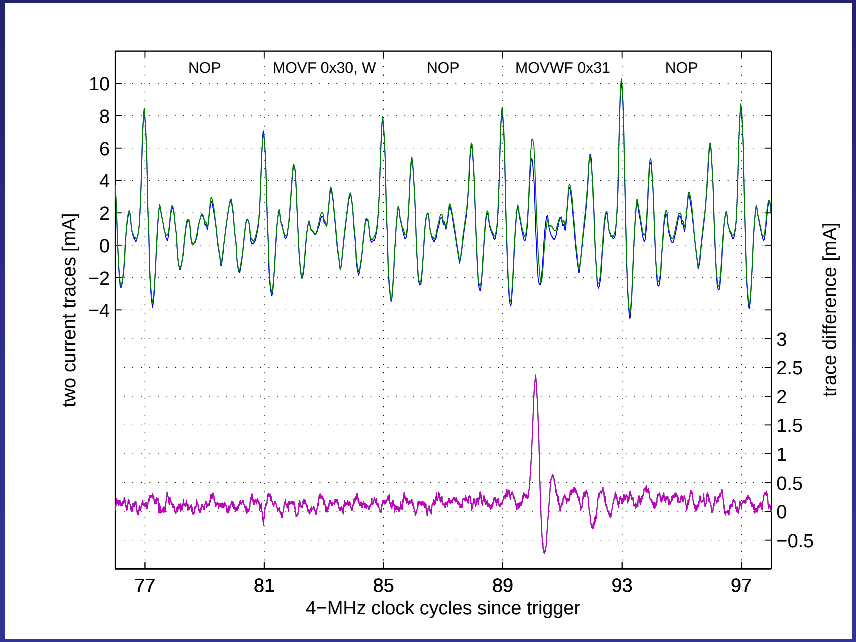


PIC16F84, Write: $(0x00 \rightarrow 0xFF) - (0x00 \rightarrow 0x7F)_L$ (Av = 1)

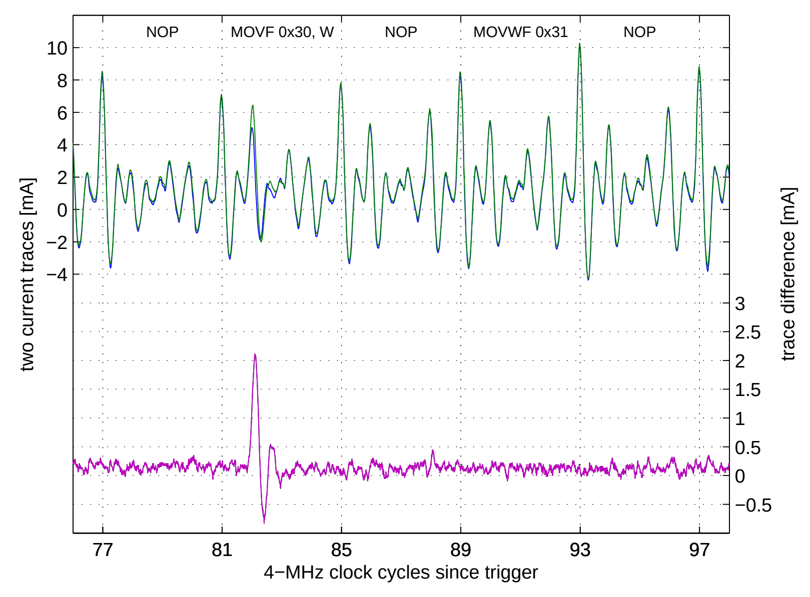
# Results

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

- State of the cell stays unchanged for low laser power
  - Response is five times higher than power analysis result for a single bit change
  - Both read and write operations can be detected
- State of the cell changes for higher laser power



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

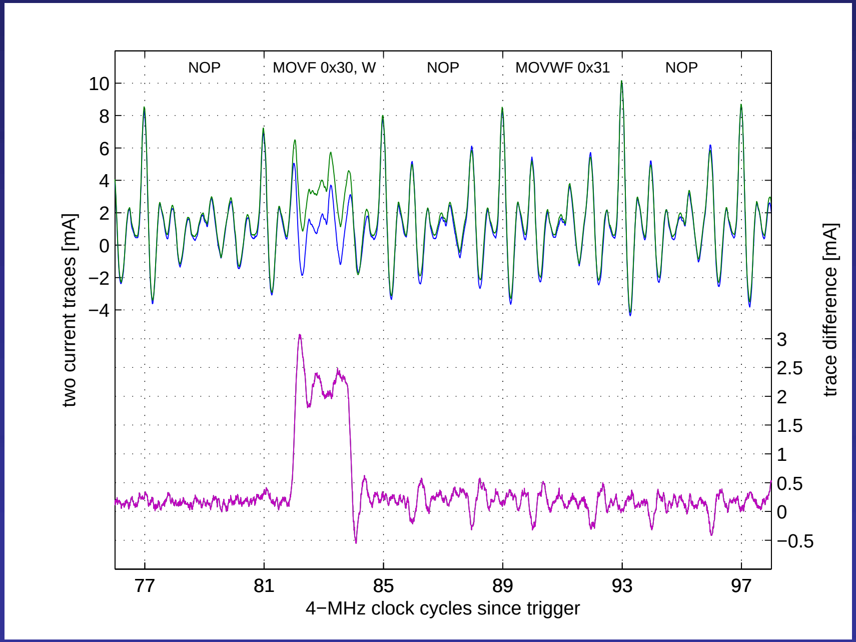


PIC16F84, Read: $(0xFF)_L$ (Av = 1)

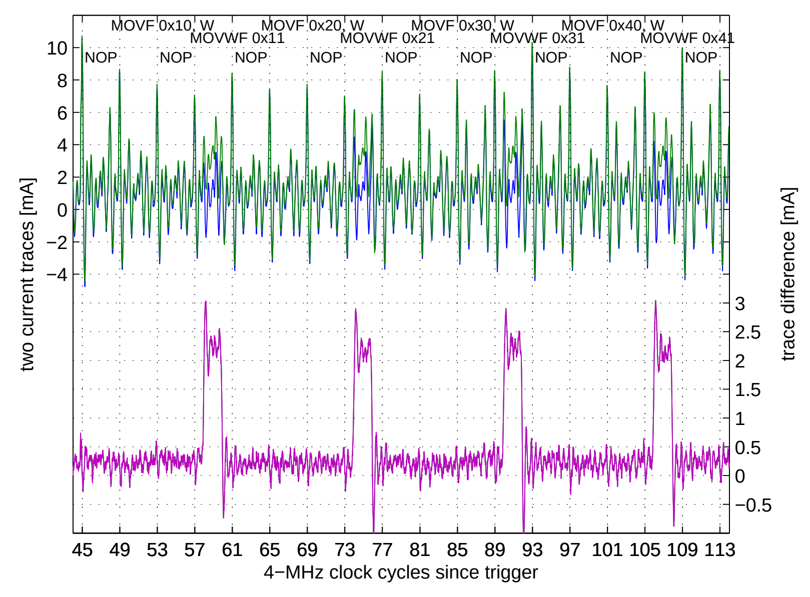
# Results

Applications for higher laser power (state changes)

- Any access to a selected cell can be detected (laser on VT1+VT4)
- Laser focused on VT3+VT6 (select transistors) of memory cell
  - Read and write operations in any cell in the whole column can be detected
- State of the memory cell changes (affect the normal chip operation)



PIC16F84, Read: $(0xFF)_L$ (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

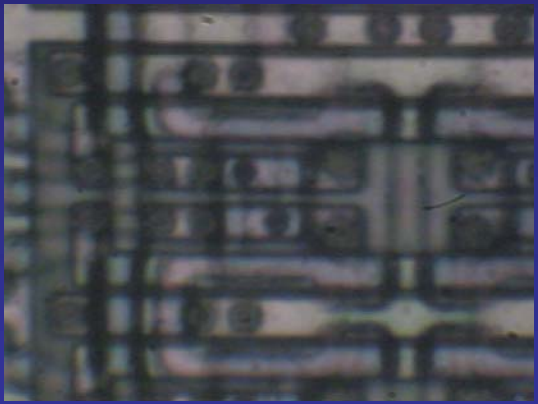
| | LIVA | ΔOBIC | SPA | OEPA |
|---|---|---|---|---|
| State of SRAM cell | OK | OK | – | OK |
| Access to SRAM cell | – | – | limited | OK |
| State change of SRAM cell | limited | OK | limited | OK |

# Improvements to the method

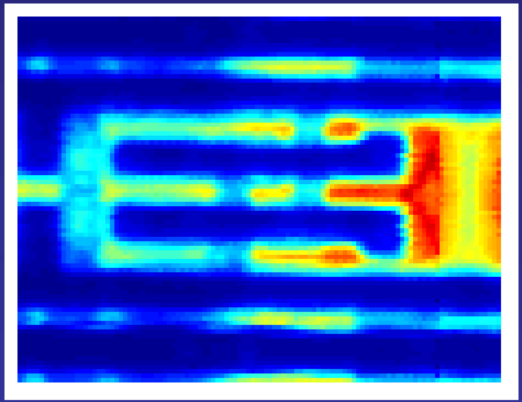
Modern chips benefit from multiple metal layers and polished insulation layers restricting optical access

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

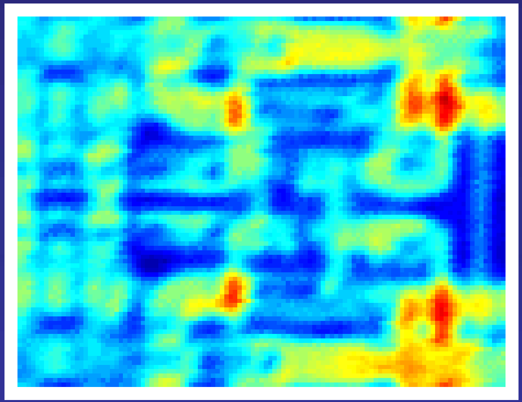
- Infrared lasers, optics and cameras must be used
- Thinning of the substrate is required for < 0.35 µm chips



PIC16F84 SRAM cell: optical image 100×



PIC16F84 SRAM cell: OBIC front image

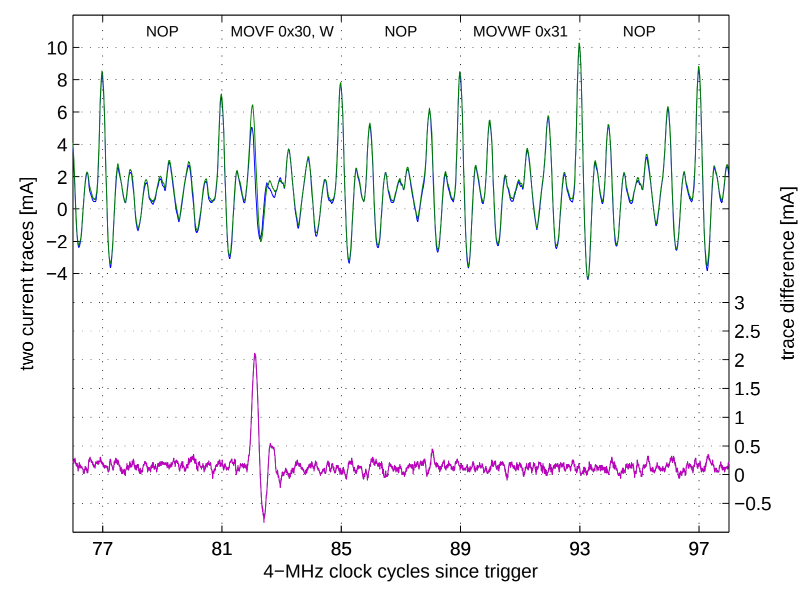


PIC16F84 SRAM cell: OBIC rear image

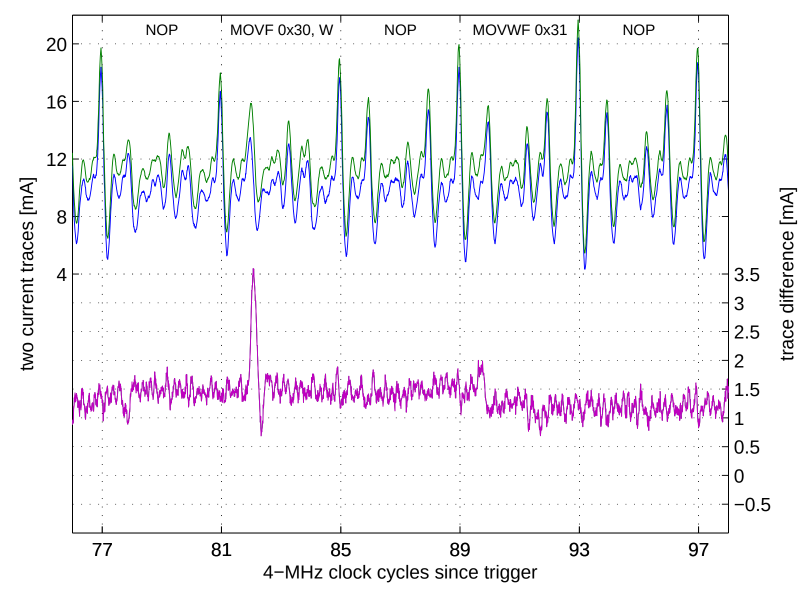
# Results for the rear-side experiments

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: $\{(0xFF)\}_L$ (Av=1)



PIC16F84 rear side, Read: $\{(0xFF)\}_L$ (Av=1)

# Conclusions

- ✓ It is possible to detect the internal state of memory cells using conventional optical probing methods
- ✓ Optically enhanced power analysis (OEPA) significantly improves the results without interfering with the device operation
- ✓ Compared to conventional power analysis, OEPA allows detection of individual bit changes
- ✓ 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
- …