Data remanence in Flash Memory Devices

Sergei Skorobogatov

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Data remanence

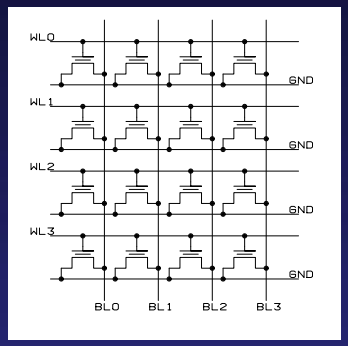
- Residual representation of data after erasure
  - Magnetic media
  - SRAM and DRAM
    - Low-temperature data remanence
    - Long-term retention effects
  - EEPROM and Flash
    - Should be possible
    - No information available
    - Independent testing was performed

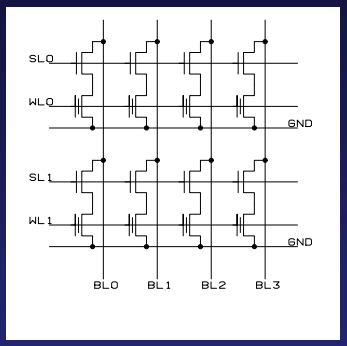
Non-volatile memories

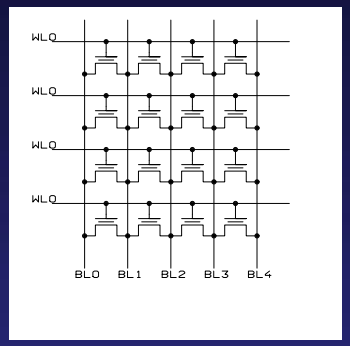
- EEPROM and Flash
  - Widely used in microcontrollers and smartcards
  - Advantages
    - Electrically programmable and erasable
    - Internal charge pumps (no external high voltages necessary)
    - High endurance (>100,000 E/W cycles)
    - Long data retention (>40 years)
  - Disadvantages
    - Larger cell size than Mask ROM
    - Flash erased in blocks
    - Longer write/erase time than SRAM

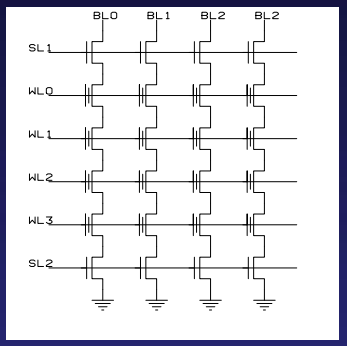
Structure of non-volatile memories

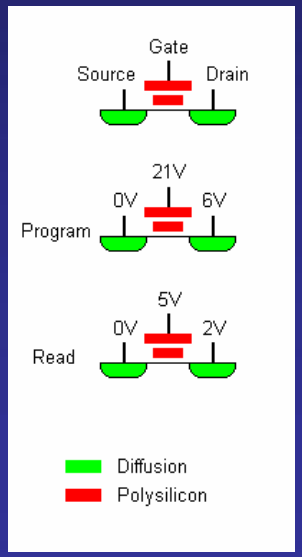
- UV EPROM
- EEPROM
- Flash EEPROM

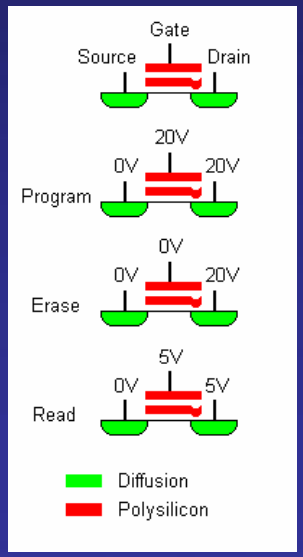


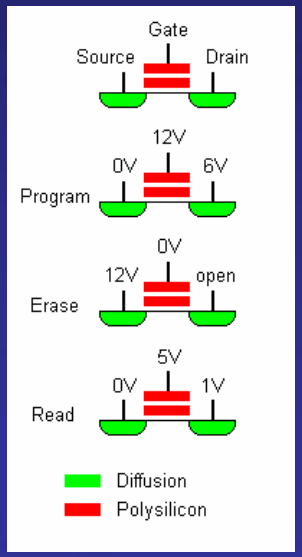


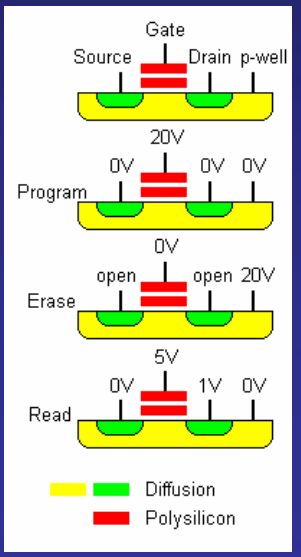










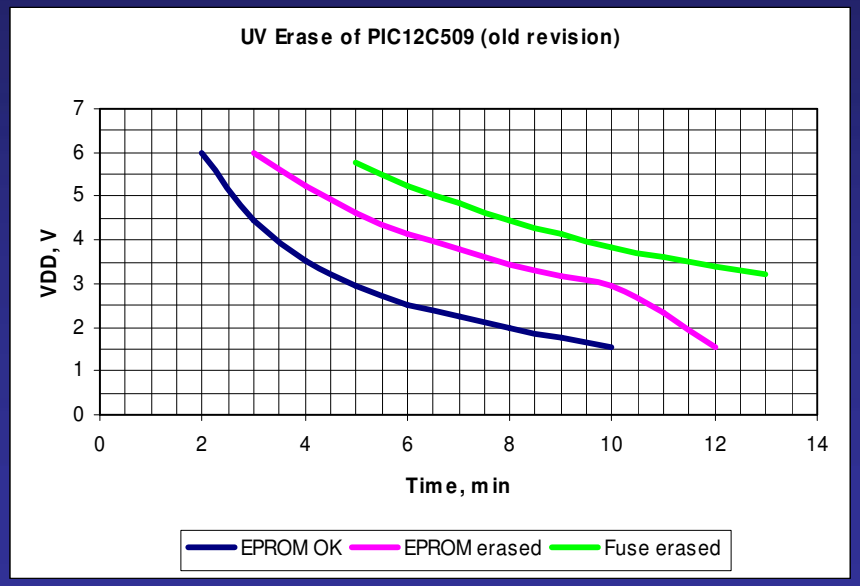


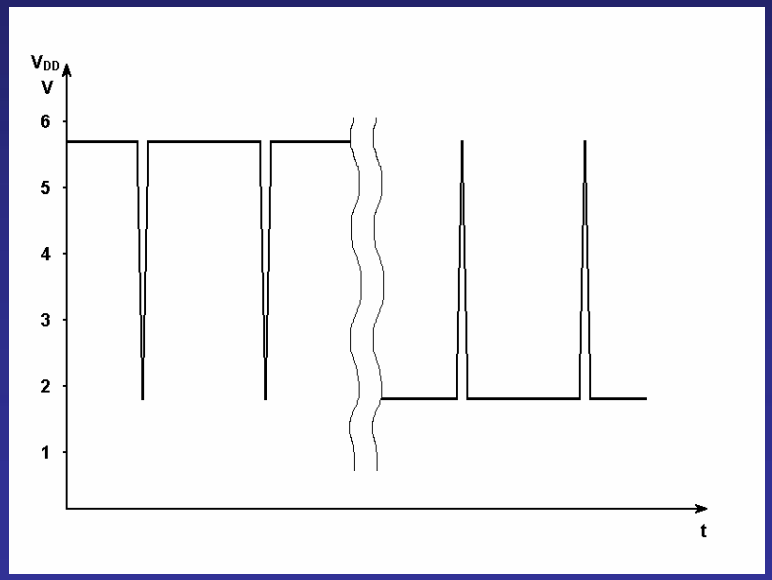
Data remanence in non-volatile memories

- EPROM, EEPROM and Flash
  - Floating-gate transistors, $10^3 – 10^5$ e^-, $\Delta V_{TH} = 3 \ldots 4$ V
- Levels of remanence threat
  - File system (erasing a file → undelete)
  - File backup (software features)
  - Smart memory (hardware buffers)
  - Memory cell
- Possible outcomes
  - Circumvention of microcontroller or smartcard security
  - Information leakage through shared EEPROM areas between different applications in smartcards

Attacks on EPROM/EEPROM devices

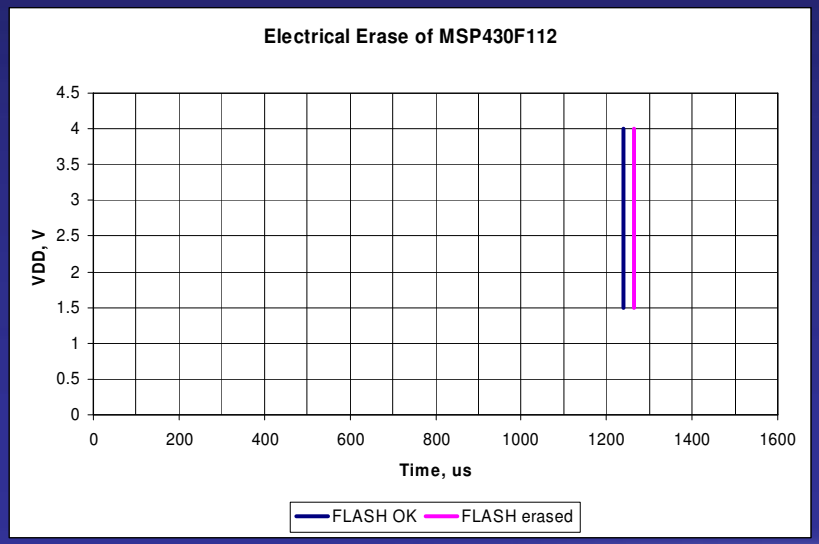
- Erase with UV light followed by power glitching
  - Memory and password/fuse are erased simultaneously
    - V_{DD} variation or power glitching
    - Read sense circuit: $V_{TH} = K\,V_{DD}$, $K \sim 0.5$
  - Not suitable for 0.35 µm and smaller technologies

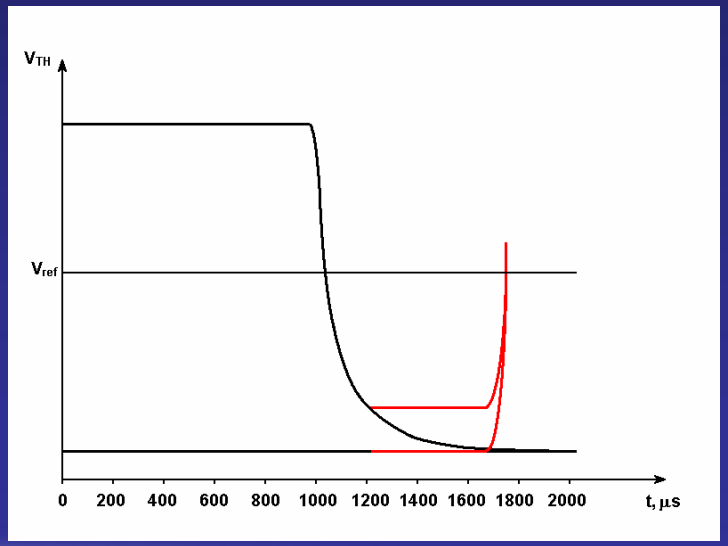




Attacks on EEPROM/Flash devices

- Electrical erase
  - Memory and password are erased simultaneously
    - Fast process (difficult to control erasure)
    - V_{TH} drops too low (power glitching does not work)
    - Cell charge alteration does not work
      - Voltage monitors and internally stabilized power supply
      - Internal charge pumps and timing control
      - Difficult to terminate the erase/programming cycle



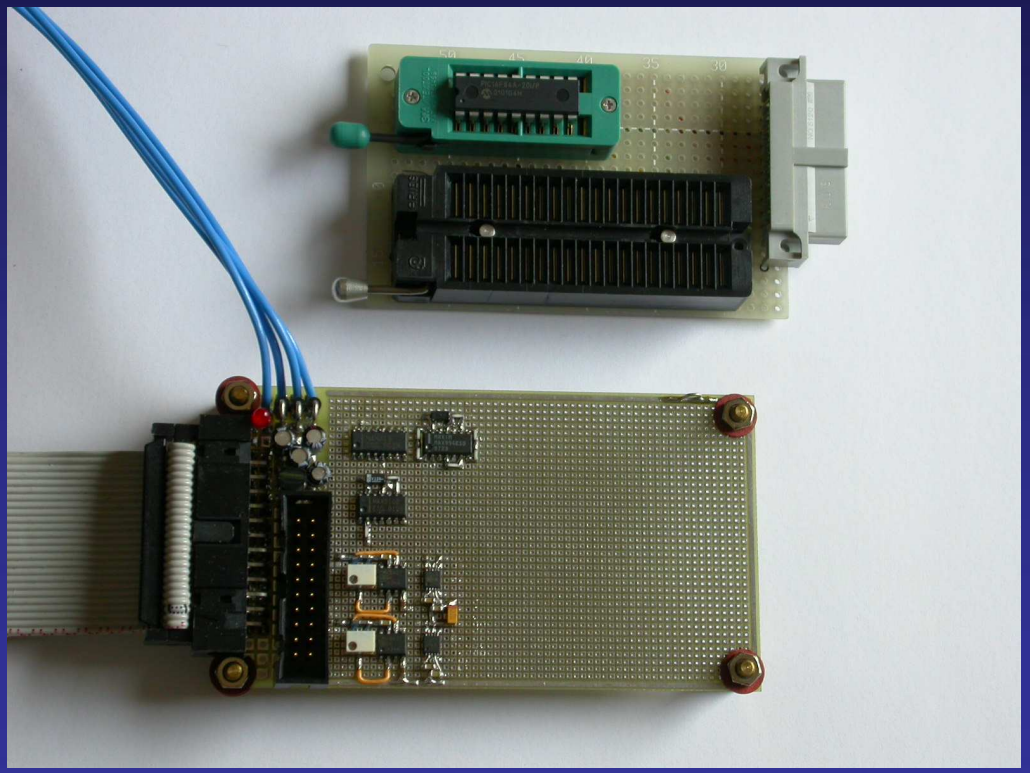


Experimental part

- Is it possible to measure a V_{TH} close to 0 V?
- Is any significant residual charge left after a normal erase operation?
- Is it possible to distinguish between never-programmed and programmed cells?
- Countermeasures?

Experimental part

- Data remanence evaluation in PIC16F84A
  - 100 µV precision power supply
  - 1 µs timing control

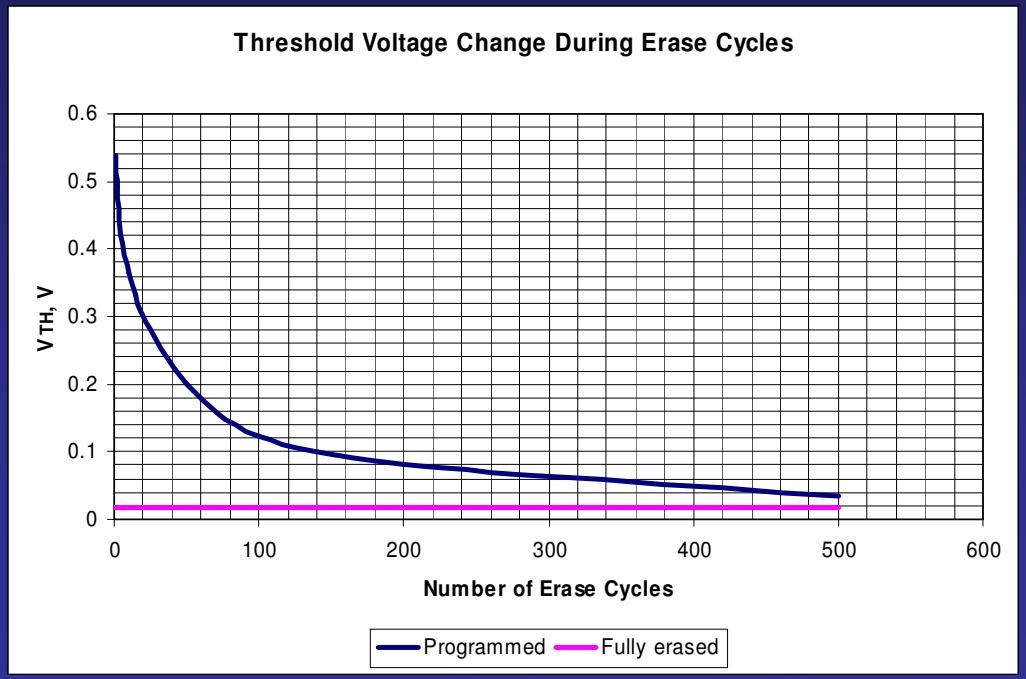


Measuring V_{TH} close to 0 V in PIC16F84A

- Power glitch to reduce V_{ref} to 0.5 V
- Exploiting after-erase discharging delay
  - Accidentally discovered 5 years ago
  - Shifts V_{TH} up by 0.6 – 0.9 V
- Apply both techniques simultaneously:
  - $V_{TH} = K\,V_{DD} - V_W$
  - $V_{TH} = -0.4 \ldots 2.0$ V

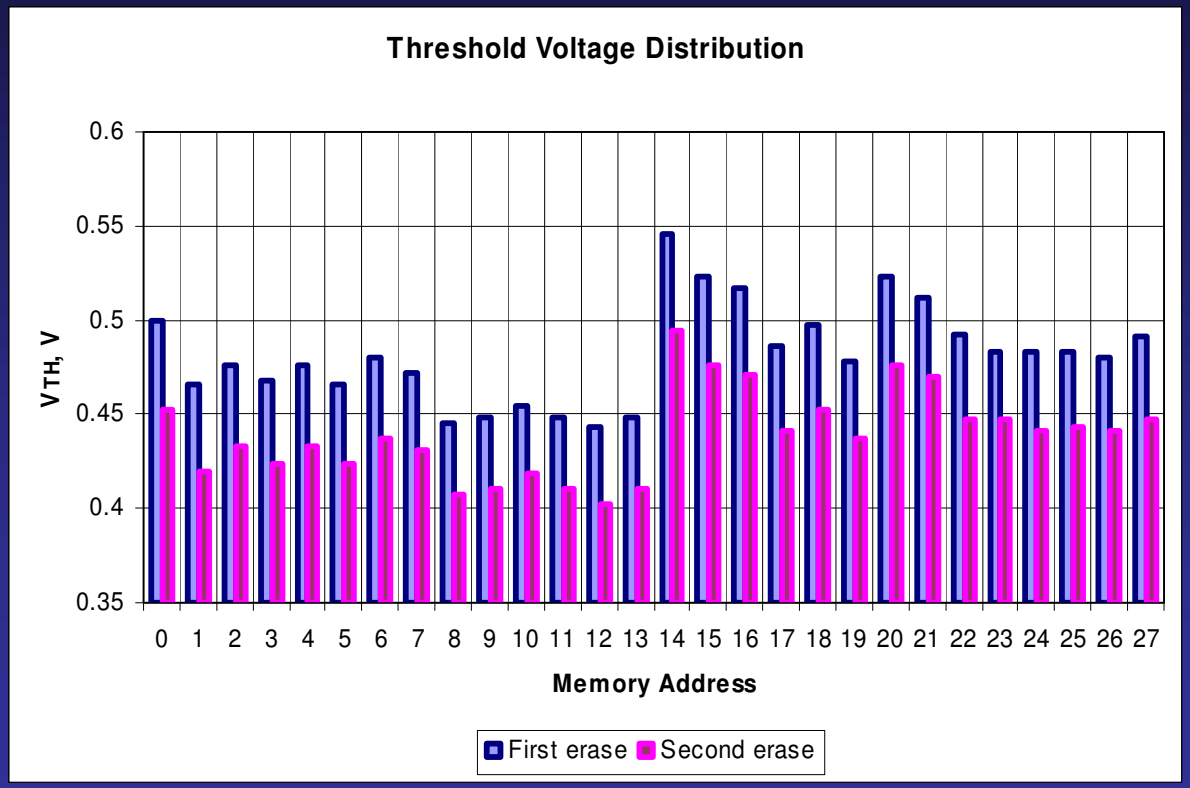
Test residual charge after erase

- $V_{TH} = V_{ref} = K\,V_{DD} - V_W$, $K = 0.5$, $V_W = 0.7$ V
- Memory bulk erase cycles (5 V, 10 ms)
  - Flash memory, 100 cycles: $\Delta V_{TH} = 100$ mV
  - EEPROM memory, 10 cycles: $\Delta V_{TH} = 1$ mV



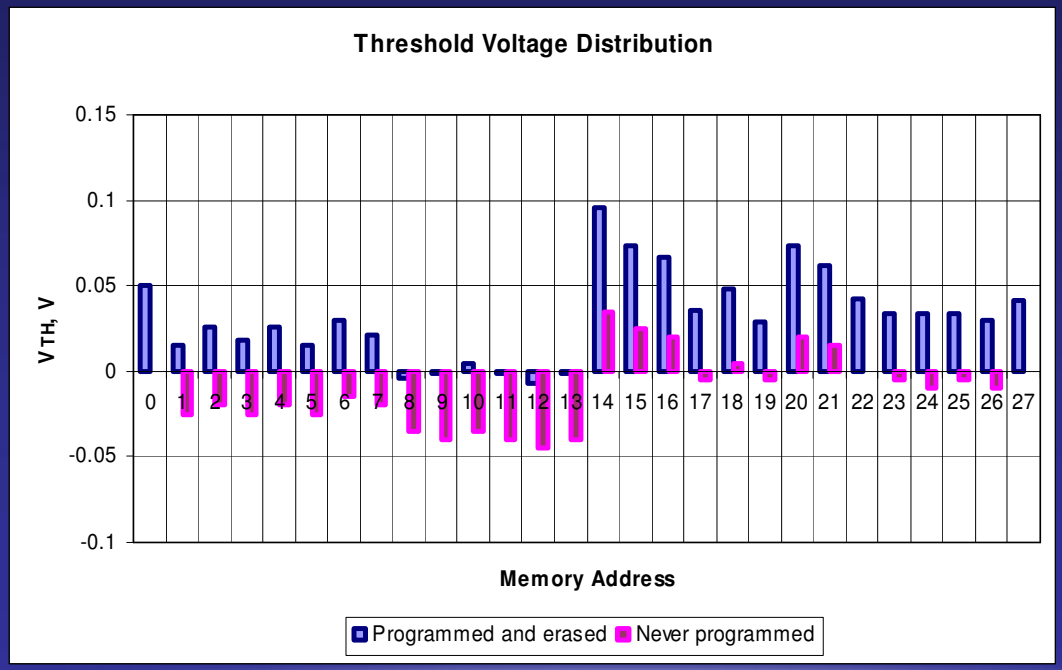
Recovering data from erased PIC16F84A

- Large difference in V_{TH} between cells in the array
- Measure the cell's V_{TH} before and after an extra erase cycle



Never-programmed and programmed cells

- PIC16F84A comes programmed to all 0's
  - 10,000 erase cycles to fully discharge cells. Measure V_{TH}
  - Program to all 0's, then another 10,000 erase cycles. Measure V_{TH}
- Still noticeable change of ΔV_{TH} = 40 mV



Programming cells before erasure

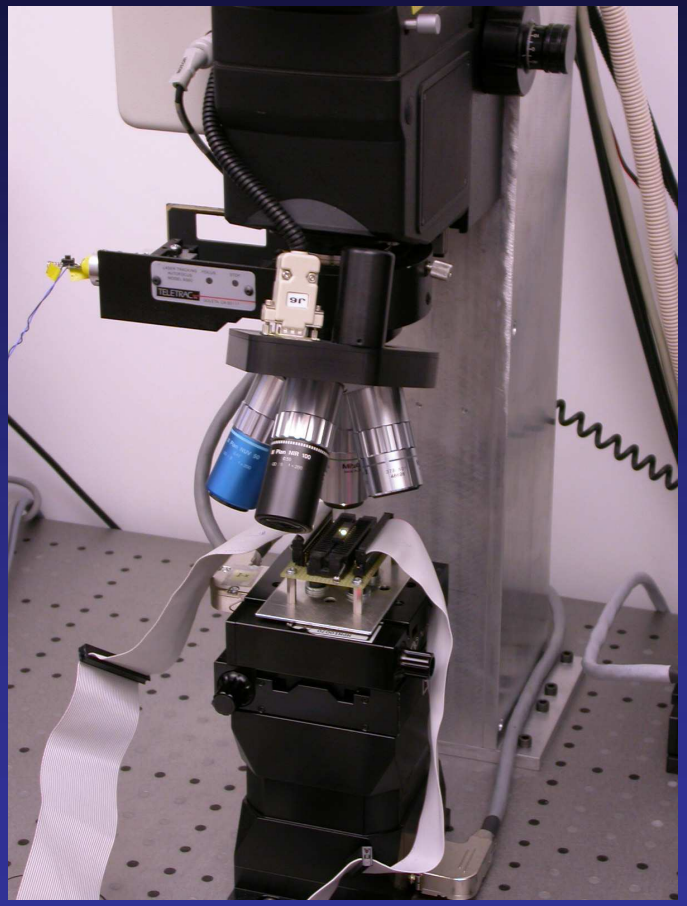
- Cannot successfully recover information from PIC16F84A if it was programmed to all 0's before the erase operation
- This is a standard procedure in some Flash and EEPROM devices:
  - Intel ETOX Flash memory (P28F010)
  - Microchip KeeLoq HCS200
- Not used in modern EEPROM/Flash memory devices

Other ways of data remanence testing

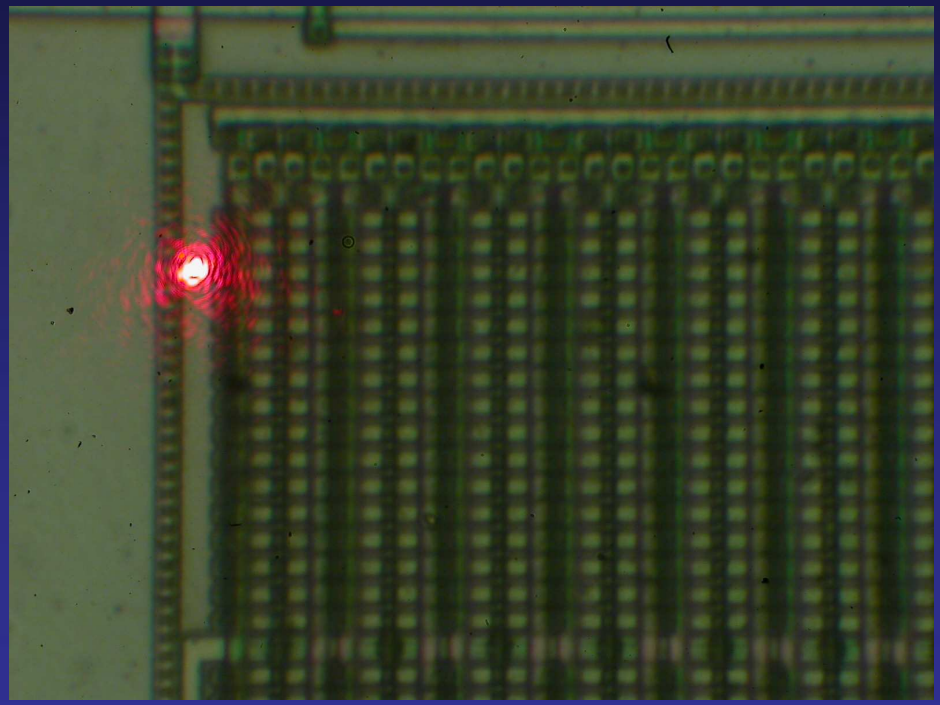
- Semi-invasive approach (access to passivation layer)
  - Measure changes inside memory transistors
  - Influence on cell characteristics (V_{TH})
  - Influence on read-sense circuit (V_{ref})
- Invasive approach (access through passivation layer)
  - Modify the read-sense circuit of the memory
  - Direct connection to internal memory lines

Semi-invasive testing

Test setup

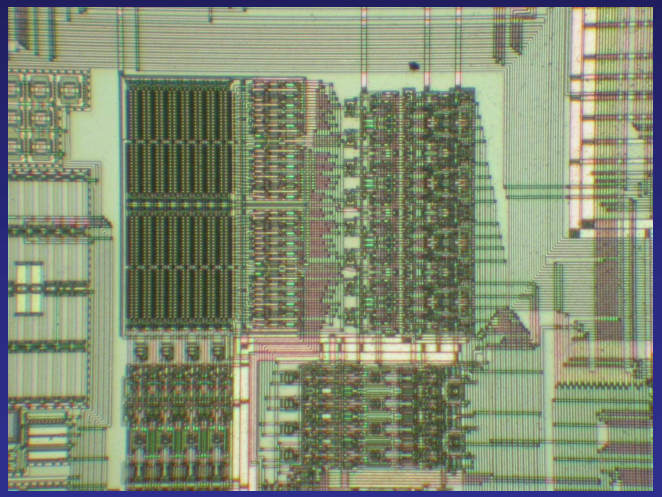


Focusing the laser (100x objective)

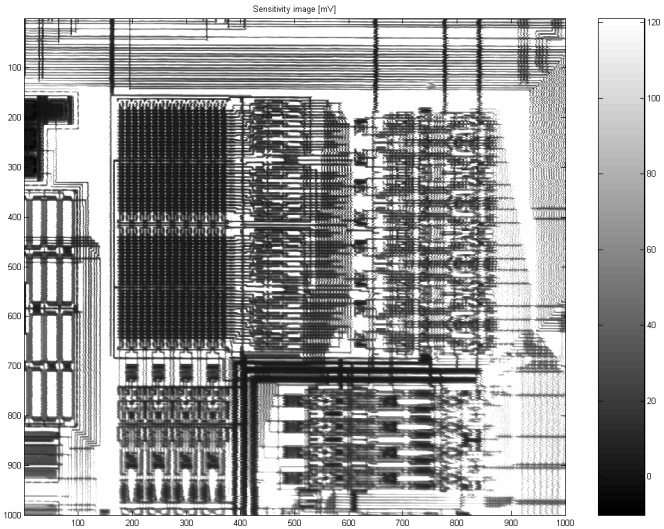


Semi-invasive testing

- Images of the PIC16F84A EEPROM (0.9 µm, 2M)
- Change $V_{ref} = f(P_L)$ to measure V_{TH}



Optical

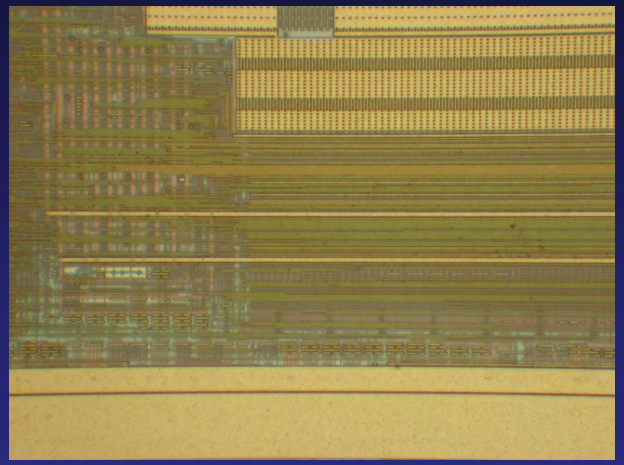


Laser scanned (OBIC)

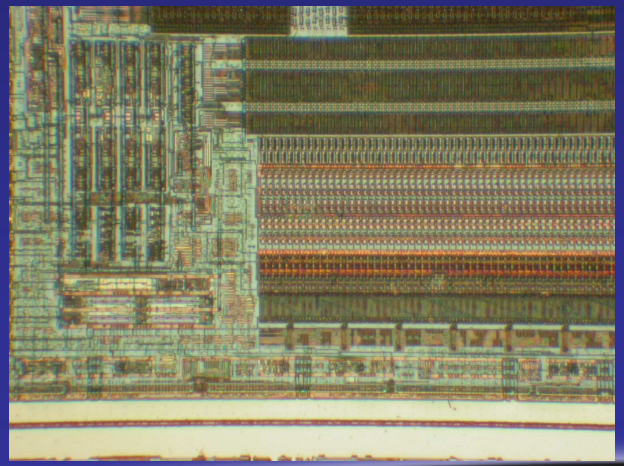
Semi-invasive testing

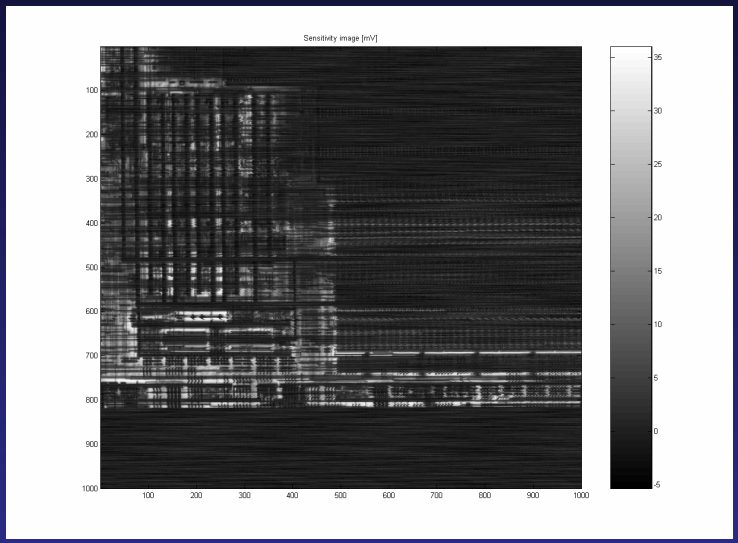
Images of the ATmega8 EEPROM (0.35 µm, 3M)

Optical



Optical after depro-cessing

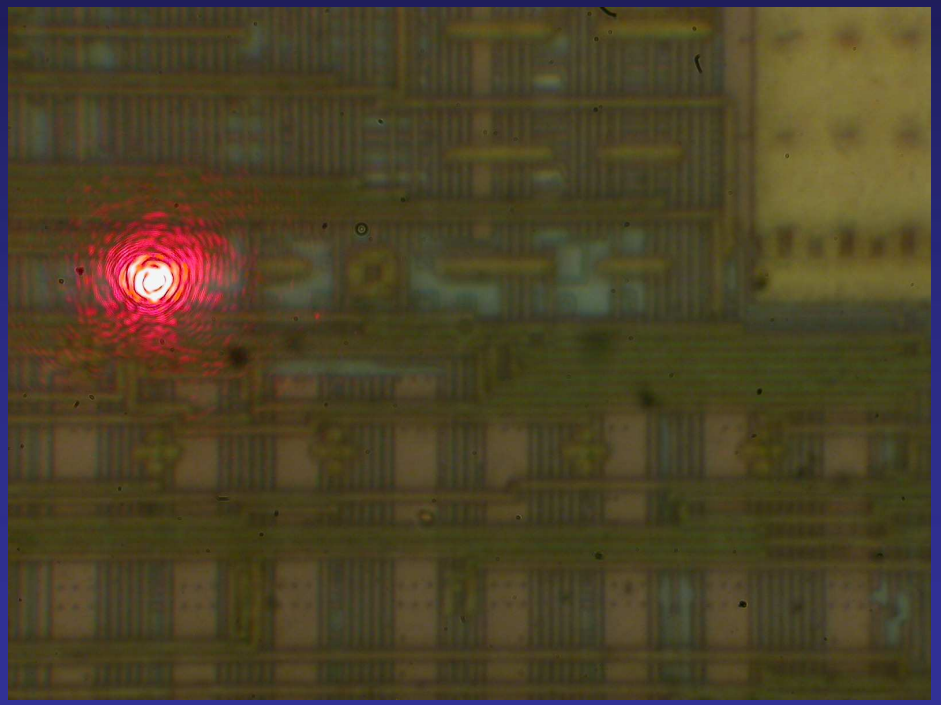




Laser scanned (OBIC)

Semi-invasive testing

- Focus a laser on the ATmega8 die using a 100x objective in order to change V_{ref}
- Less successful (<10% after one erase cycle) due to multiple metal layers and polished insulation layers



Countermeasures

- Cycle EEPROM/Flash 10 – 100 times with new random data before writing sensitive information to them
- Program (charge) all EEPROM/Flash cells before erasing them
- Remember about “intelligent” memories, backup and temporary files in file systems
- Remember that memory devices are identical within the same family:
  - everything which is valid for PIC16F84A will work for PIC16F627/628, PIC16F870/871/872 and PIC16F873/874/876/877
- Use latest high-density devices, as smaller scales make semi-invasive attacks less feasible
- Cryptography can help to make data recovery more difficult. E.g. store longer pre-key R instead of key: K=h(R)

Conclusions

- Floating-gate memories (EPROM, EEPROM and Flash) have data-remanence problems
- Information from some samples can be recovered even after 100 erase cycles
- Even where the residual charge cannot yet be detected with existing methods, future technologies may permit this
- Secure devices should be tested for data-remanence effects