Data remanence in non-volatile semiconductor memories

Part I: Introduction and non-invasive approach

Sergei Skorobogatov

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Data remanence

- Magnetic media
- SRAM and DRAM
  - Low temperature data remanence
  - Long-term retention effects
  - Burning-in data
- Data retention
  - Connected to remanence
  - Specified by manufacturers

Data remanence in non-volatile memories

- EPROM, EEPROM and Flash
  - Floating-gate transistors, 10^3 - 10^5 ē, $\Delta V_{TH} = 3.5$ V
- Levels
  - File system (erasing a file)
  - File backup (software features)
  - Smart memory (hardware buffers)
  - Memory array
- Possible threats
  - Resetting security protection in microcontrollers
  - Sharing EEPROM area between different applications in smartcards

Non-volatile memories

- UV EPROM
  - Advantages
    - Electrically programmable
    - Compact design (1T cell)
  - Disadvantages
    - Long write time (>10 ms)
    - High voltages for programming
    - Very long erase time (>10 min) and UV light use
    - Not scalable below 0.35 μm (top metal layers)
    - High cost (quartz window in ceramic) or OTP
    - Low endurance (100 E/W cycles)
    - Short data retention (10 years)

Non-volatile memories

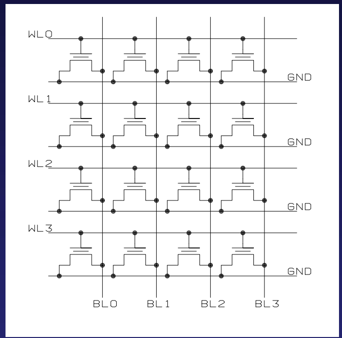
- EEPROM
  - Advantages
    - Electrically programmable and erasable
    - Internal charge pumps in modern devices
    - High endurance (>100,000 E/W cycles)
    - Long data retention (>40 years)
  - Disadvantages
    - Large cell size (2T cell)
    - Long write time (>1 ms) and erase time (>100 ms)
    - High voltages for programming (old designs)
    - High cost (low density)

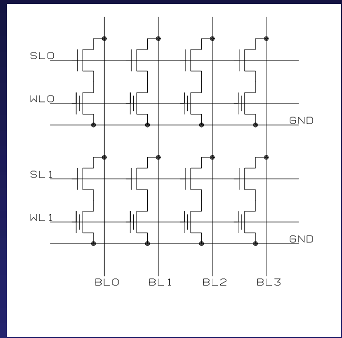
Non-volatile memories

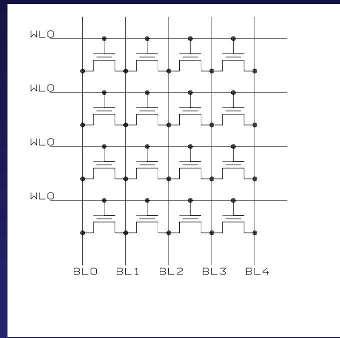
- Flash EEPROM
  - Advantages
    - Electrically programmable and erasable
    - Internal charge pumps
    - Compact design (1T cell)
    - Fast write time (1 - 100 μs)
    - High endurance (>100,000 E/W cycles)
    - Long data retention (>100 years)
    - Low cost (compact design, 0.13 μm and smaller)
  - Disadvantages
    - Erasing in blocks
    - Long erase time (>100 ms)

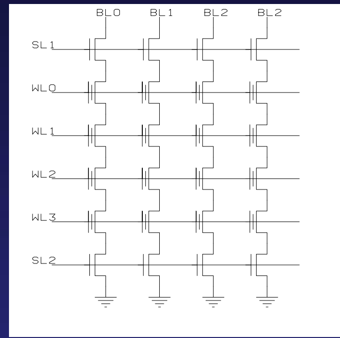
Structure of non-volatile memories

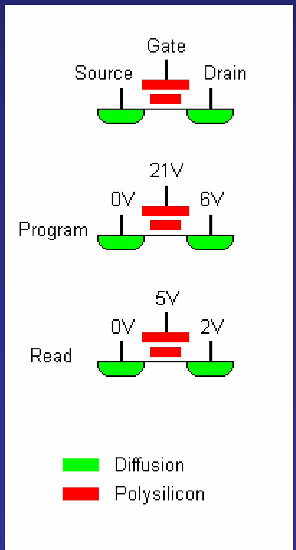
- UV EPROM EEPROM Flash EEPROM

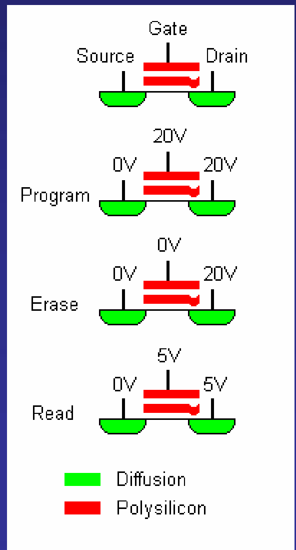


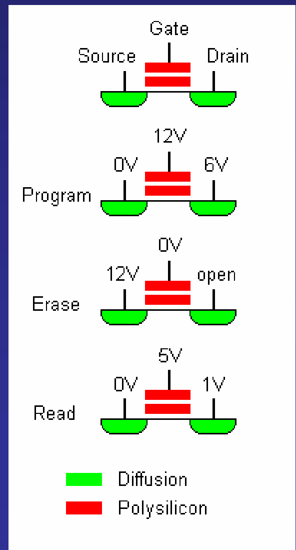


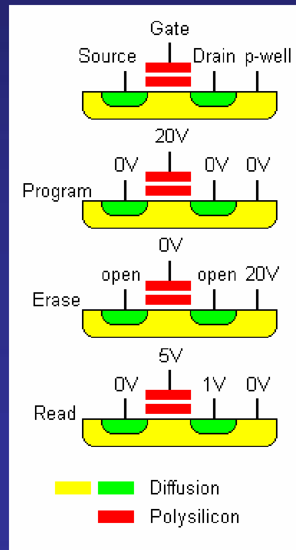












Security in EPROM devices

- Security fuse location
  - Separate from main memory
  - Embedded in main memory
- Security monitoring
  - On reset or initialisation
  - Each time access is requested
  - Permanent
- Protection from UV light
  - Top metal layer
  - Fuses embedded in main memory

Security in EPROM devices

- Erasing with UV light
  - Memory and fuse are erased simultaneously
  - Memory is erased before the fuse

Security in EEPROM/Flash devices

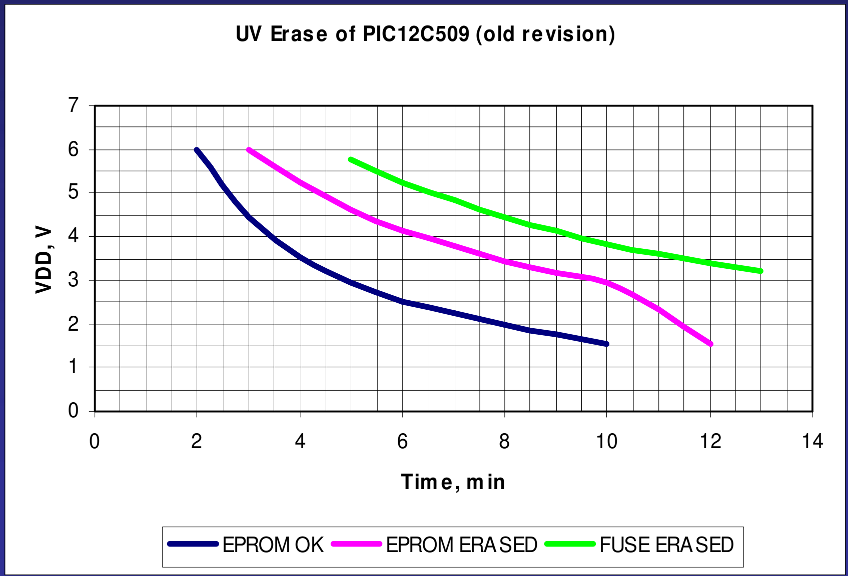
- Security fuse location
  - Separate from main memory
  - Embedded in main memory
- Security monitoring
  - On reset or initialisation
  - Each time access was requested
  - Permanent
- Protection
  - Top metal layer from UV light
  - Inverted cells or non-sensitive to UV light
  - Passwords

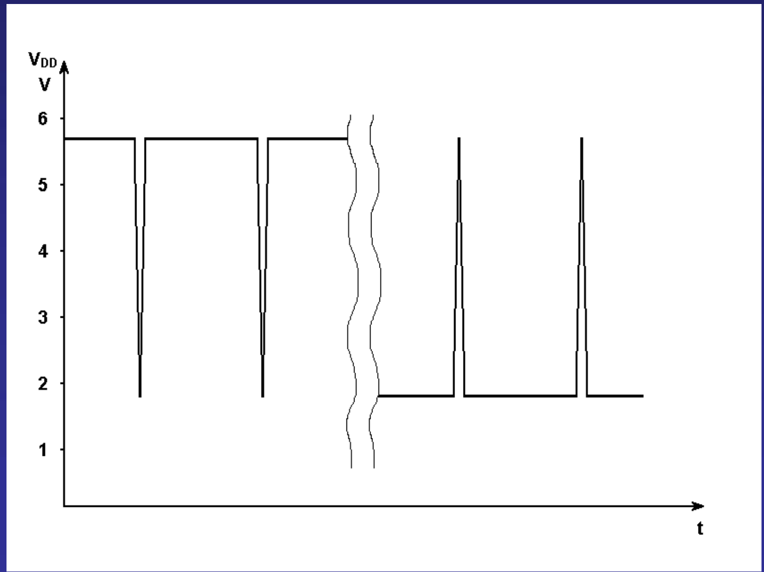
Security in EEPROM/Flash devices

- Electrical erase
  - Fuse is erased before the memory
  - Memory and fuse are erased simultaneously
  - Memory is erased before the fuse

Attacks on EPROM devices

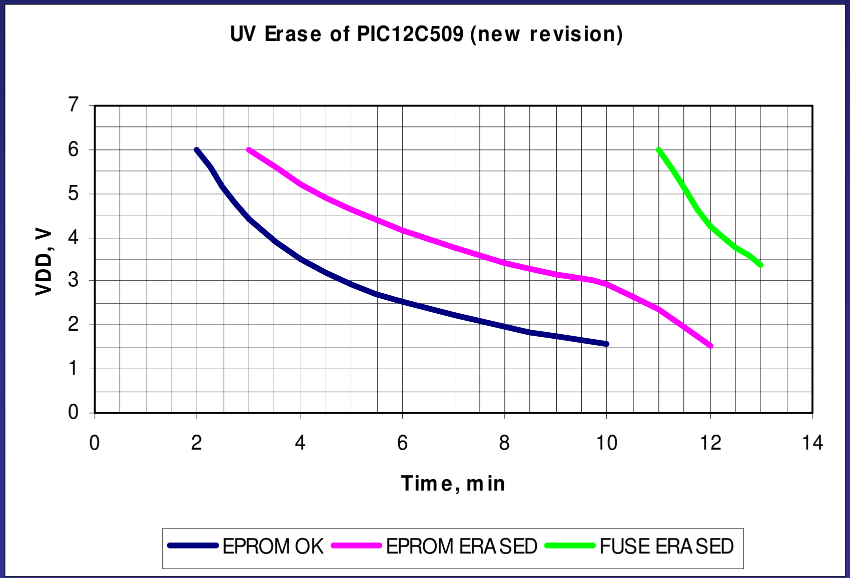
- Erasing with UV light
  - Memory and fuse are erased simultaneously
    - V_{DD} variation or power glitching
    - Read sense circuit: $V_{TH} = K\ V_{DD}$, K ~ 0.5

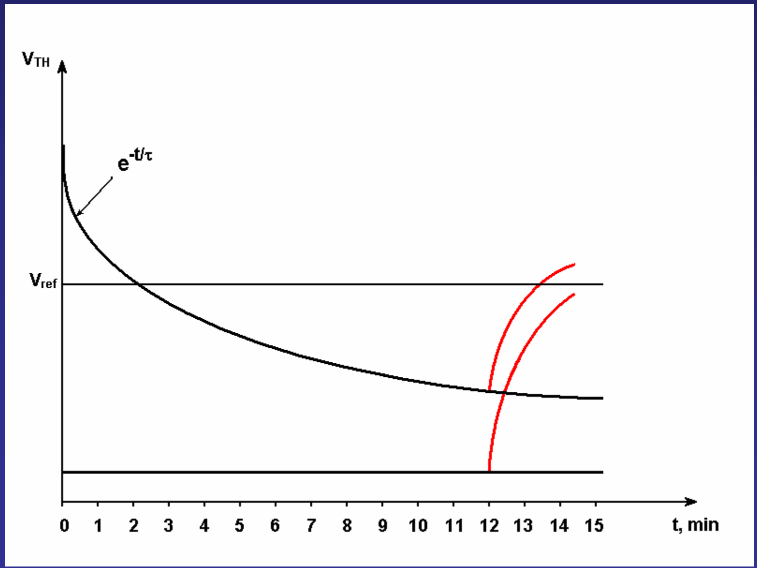




Attacks on EPROM devices

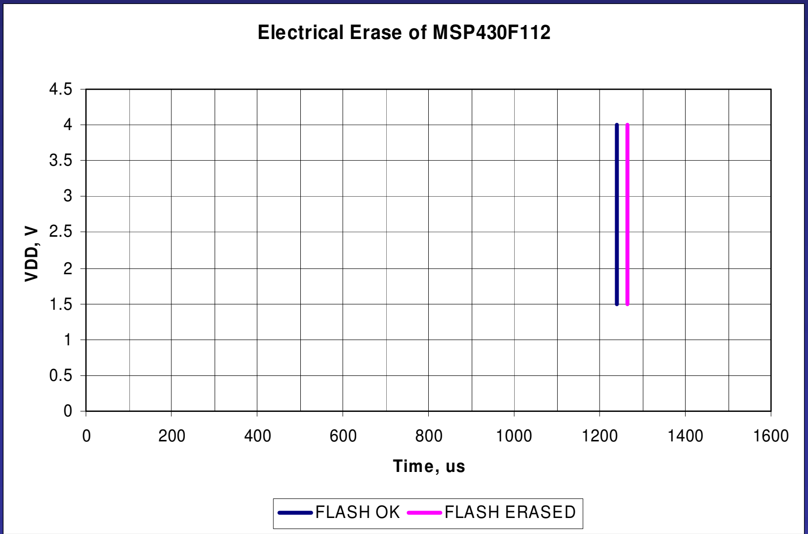
- Erasing with UV light
  - Memory is erased before the fuse
    - Cell charge alteration (controlled CHE injection)
    - External control over programming parameters

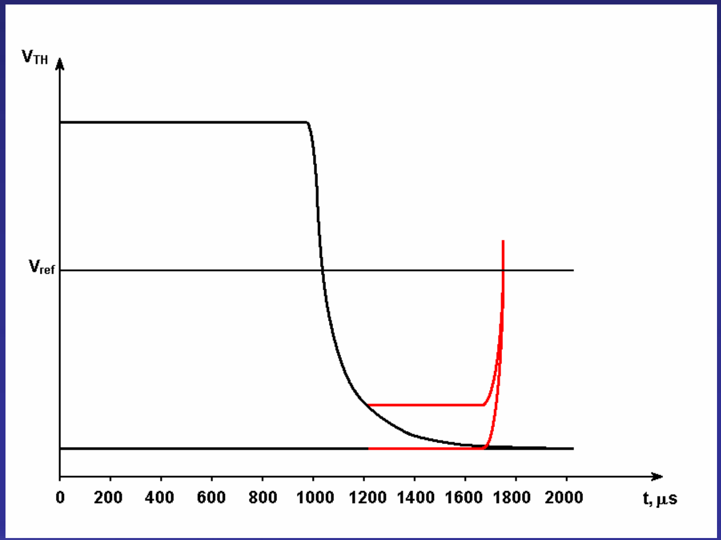




Attacks on EEPROM/Flash devices

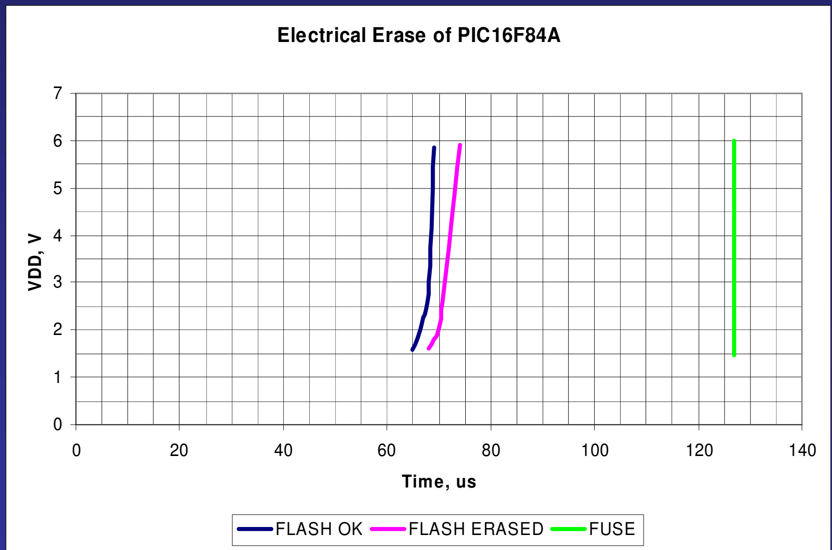
- Electrical erasing
  - Memory and fuse are erased simultaneously
    - Fast process (difficult to control erasing)
    - V_{TH} drops too low (power glitching does not work)
    - Internally stabilized power supply and voltage monitors
    - Cell charge alteration does not work
      - Internal charge pumps and timing control
      - Fowler-Nordheim tunneling or fast CHE injection

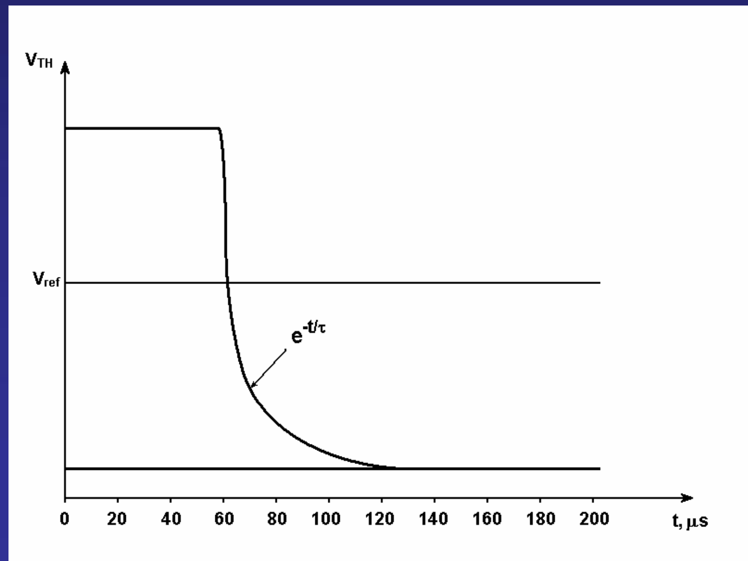




Attacks on EEPROM/Flash devices

- Electrical erasing
  - Memory is erased before the fuse
    - Five times excess in PIC16F84A
    - $q = q_0\ e^{-t/\tau}$, $\tau = 5\ \mu s$: $10^5\ \bar{e} \rightarrow 1 - 2\ \bar{e}$
    - Standard erase cycle = 10 ms



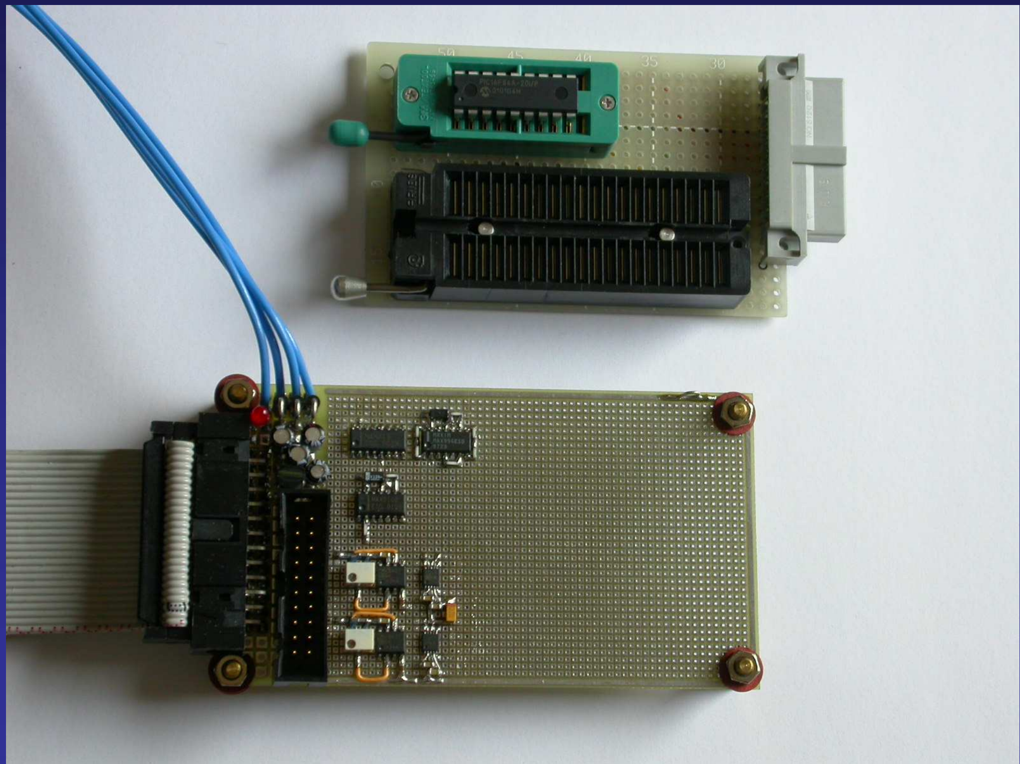


Experimental part

- Test whether it is possible to measure V_{TH} close to 0 V
- Test whether any significant residual charge is left after normal erase operation
- Test whether it is possible to distinguish between never-programmed and programmed cells
- Work out suggestions and countermeasures if necessary

Experimental part

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

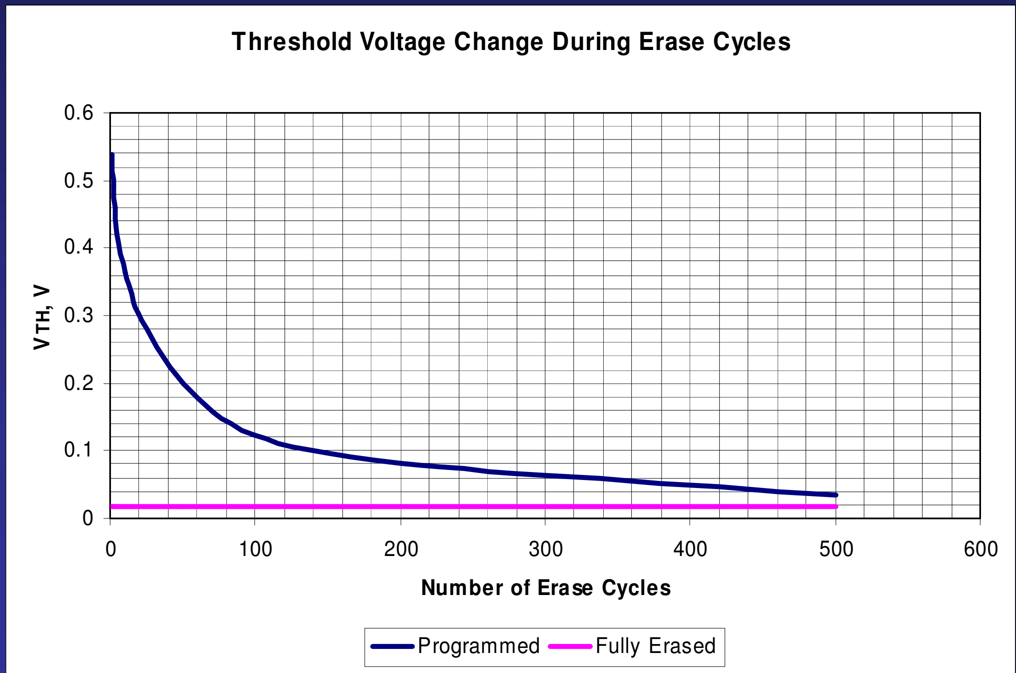


Measuring V_{TH} close to 0 V in PIC16F84A

- Using power glitching technique
  - Reducing V_{ref} to 0.5 V
- Exploiting after-erase discharging bug
  - Accidentally discovered 5 years ago
  - Shifts V_{TH} up by 0.6 - 0.9 V
- Applying both techniques simultaneously
  - $V_{TH} = K\ V_{DD} - V_W$
  - $V_{TH} = -0.4$ - 2.0 V

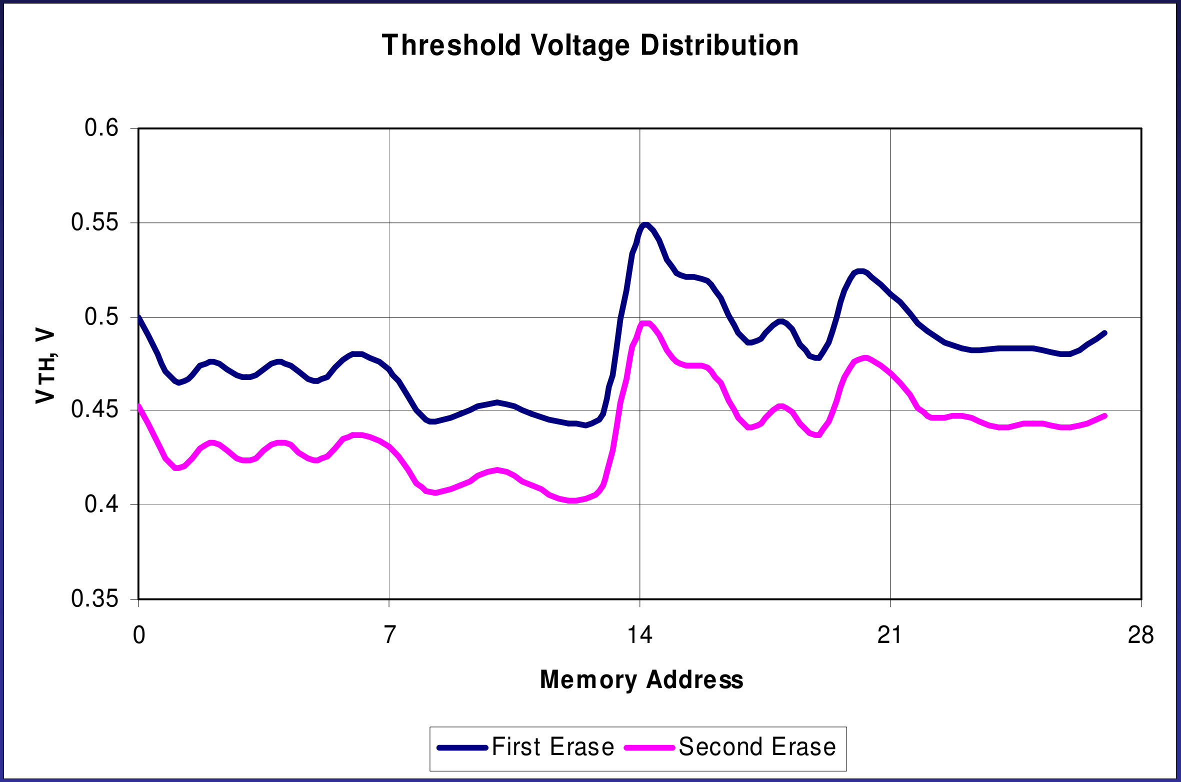
Test residual charge after erase

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



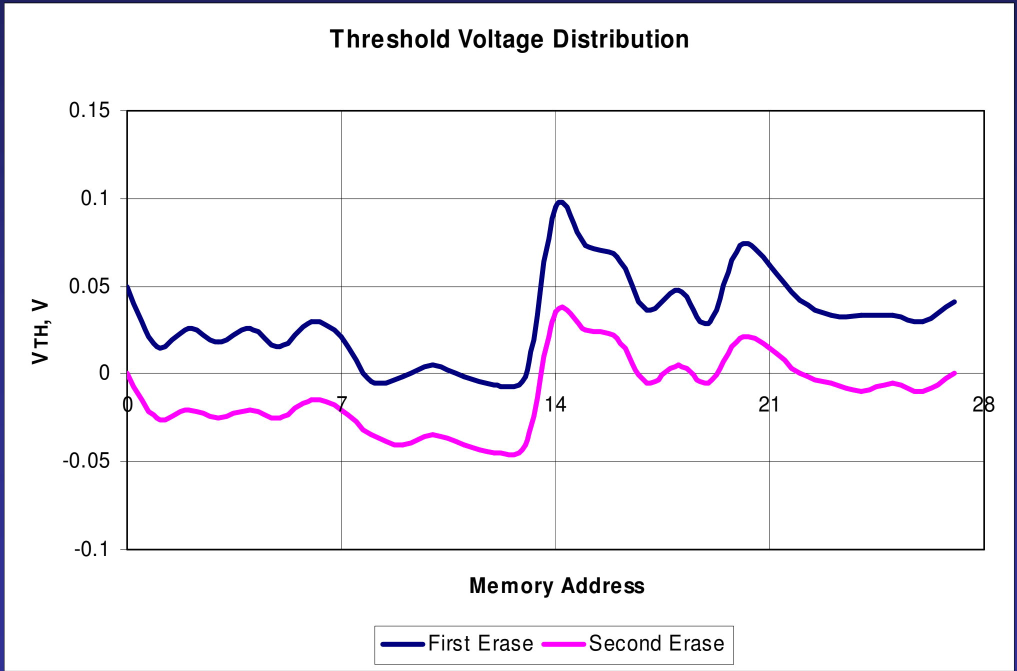
Recovering data from erased PIC16F84A

- Large difference in V_{TH} between cells in the array
- Reference to the cell itself after an extra erase cycle



Never-programmed and programmed cells

- PIC16F84A comes programmed to all 0's
  - 10,000 erase cycles and 10 hrs at 150˚C
  - Program all 0's, then 10,000 erase cycles
- Still noticeable change of V_{TH} = 40 mV



Programming cells before erasing

- No successfully recovered information from PIC16F84A if it was programmed with all 0's before the erase operation
- Used as a standard in some Flash and EEPROM devices
  - Intel ETOX Flash memory (P28F010)
  - Microchip KeeLoq HCS200

Countermeasures

- Cycle EEPROM/Flash 10 – 100 times with random data before writing anything sensitive to them
- Program all EEPROM/Flash cells before erasing them
- Remember about too intelligent memories, backup/temporary files and 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 which benefit from newest technologies
- Using encryption helps make data recovery more difficult

Further research

- Back to the subtitle of this talk
  - Part I: Introduction and non-invasive approach
  - Good for security – less than 5% of memory devices are susceptible to non-invasive attack discussed in this talk
- Semi-invasive approach
  - Measuring changes inside memory transistors
  - Influence on cell characteristics
  - To be Part II
- Invasive approach
  - Modifying the read sense circuit of the memory
  - Direct connection to the internal memory lines
  - To be Part III

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 if the residual charge cannot be detected with existing methods it might be possible in the future with new technologies
- Secure devices should be tested for any possible outcomes of data remanence effect