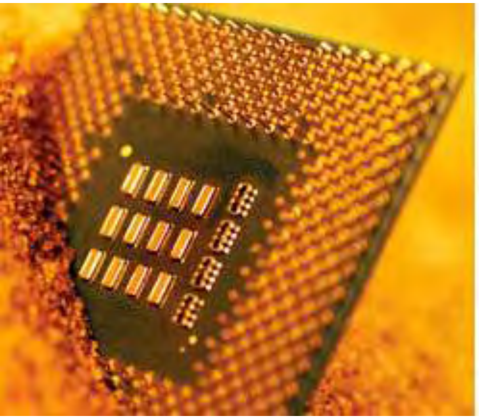
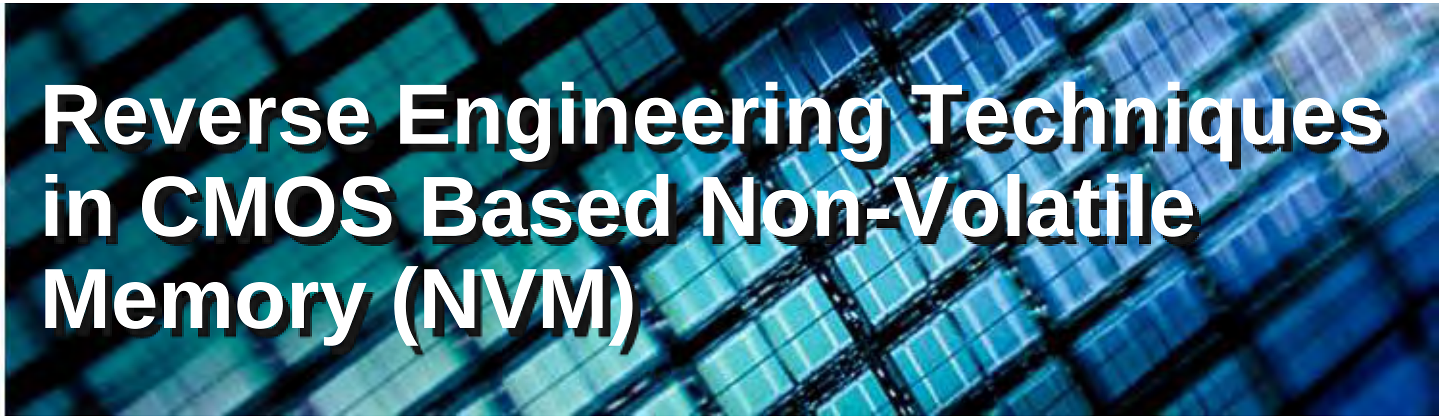




Reverse Engineering Techniques in CMOS Based Non-Volatile Memory (NVM)

EMBEDDED SRAM & NVM | LOGIC LIBRARIES | EMBEDDED T&R | MEMORY DEVELOPMENT SW | INTERFACE IP

Agenda

- Applications Requiring Standard CMOS NVM
- Technology Comparison
  - Floating Gates
  - Antifuse / Oxide Rupture
- Sample Preparation
- Reverse Engineering Techniques
  - Physical Inspection
  - Electrical Inspection
- Conclusions

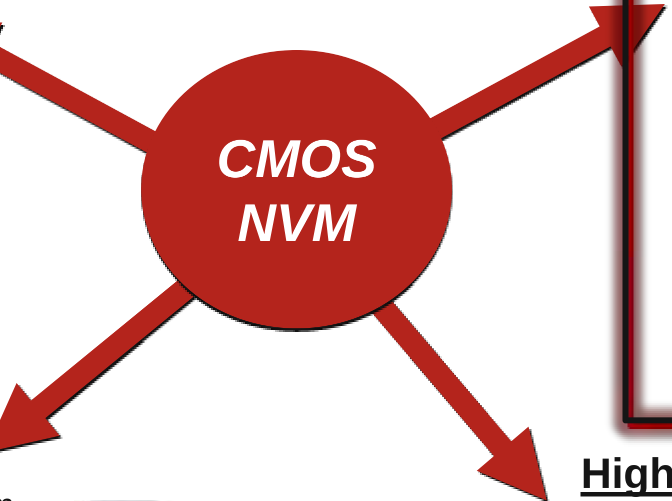
Standard CMOS NVM

Markets & Applications

Wireless / RF

Uses
- Configuration settings
- EEPROM replacement
- Customer settings (i.e. volume)

Markets
- 802.11
- BlueTooth
- Zigbee
- GPS
- RFID



Security / Encryption

Uses
- Encryption keys
- Counters

Markets
- Flash controllers
- Hard disk drives
- Home entertainment devices (HDMI)
- Digital content devices

Analog

Uses
- Post package trim
- Fuse replacement
- In-field calibration

Markets
- Precision analog (i.e. ADCs)
- Silicon Clocks
- MEMS pressure sensors
- Accelerometers / gyroscopes

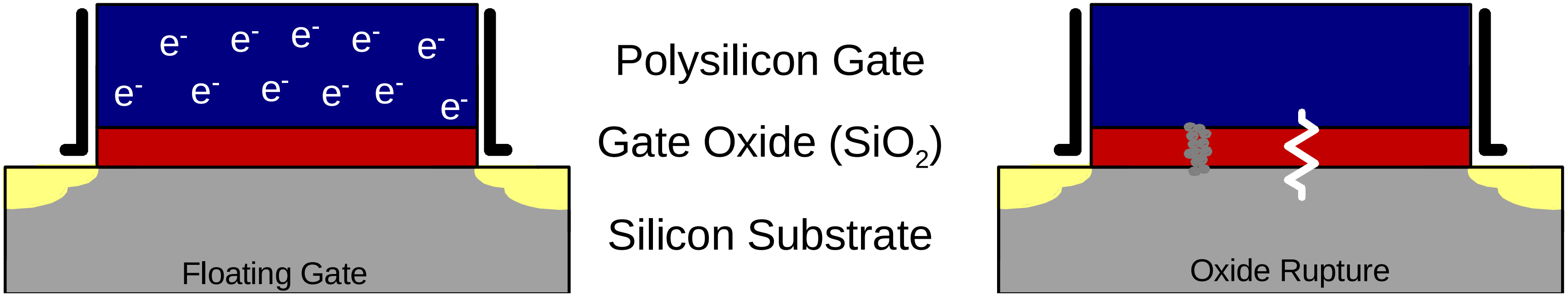
High Reliability

Uses
- Real time status and control
- Configuration settings

Markets
- Power management
- Automotive
- Military

Standard CMOS NVM

Technology Comparison

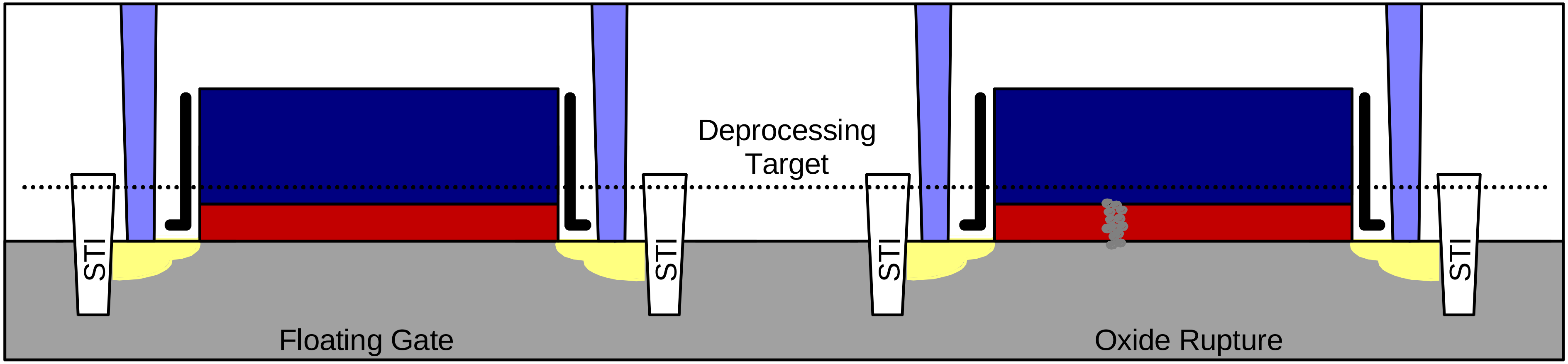


- **Floating Gate**
  - Similar to Flash / EEPROM technology
  - Charge added / subtracted using tunneling or injection
  - Multiple time programmable capability
  - Data is read based on Vt shift of device

- **Antifuse**
  - Also called oxide rupture
  - Microscopic damage done to gate oxide due to overstress
  - One time programmable only
  - Data is read based on leakage of programmed vs. unprogrammed cells

Reverse Engineering CMOS NVM

Sample Preparation

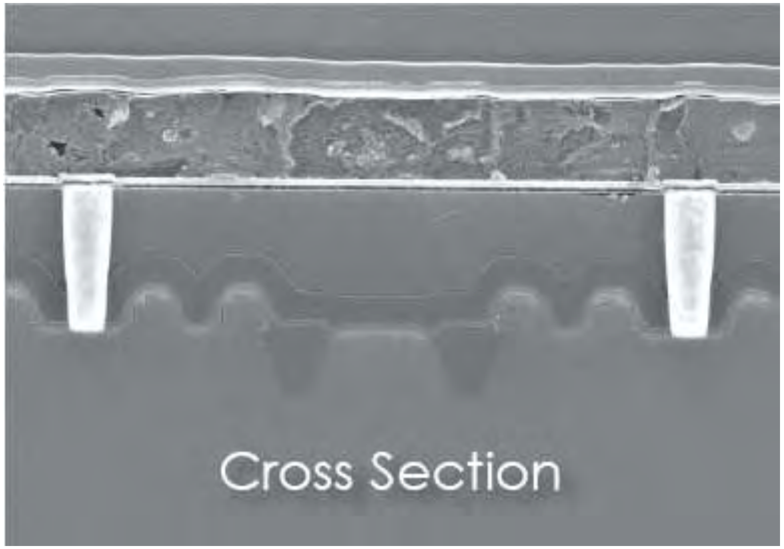


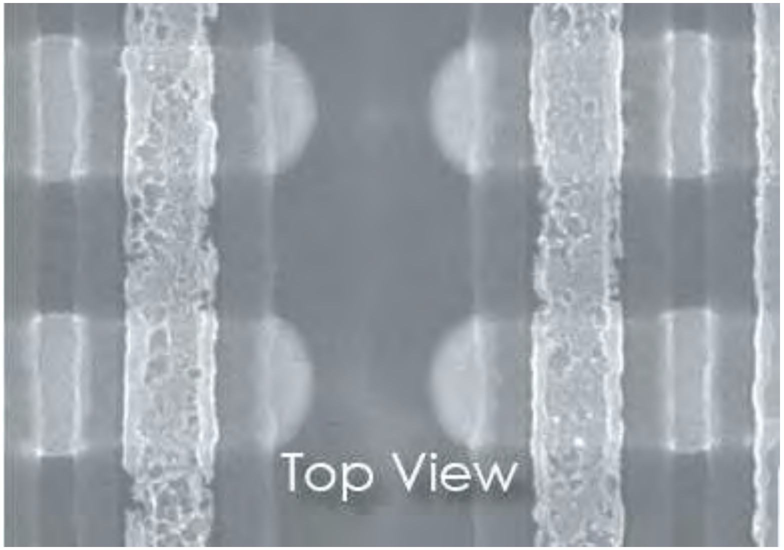
- Both technologies target deprocessing down to the polysilicon layer for any electrical techniques
- Floating gates
  - No plasma etch steps allowed during reprocessing
    - Any charged particles may disturb the state of the floating gate
  - Only wet etch is allowed
  - Deprocessing to the polysilicon exposes the charge storage layer
- Antifuse
  - Immune to most deprocessing techniques
    - Data does not get compromised / disturbed easily
  - Some techniques may require deprocessing all the way to the gate oxide layer

Reverse Engineering CMOS NVM

Physical Inspection

- Standard physical inspection (cross section / top level) does not work for either technology
  - Floating gates leave no physical imprint on the silicon
  - Antifuse damage is too small / localized to be found effectively



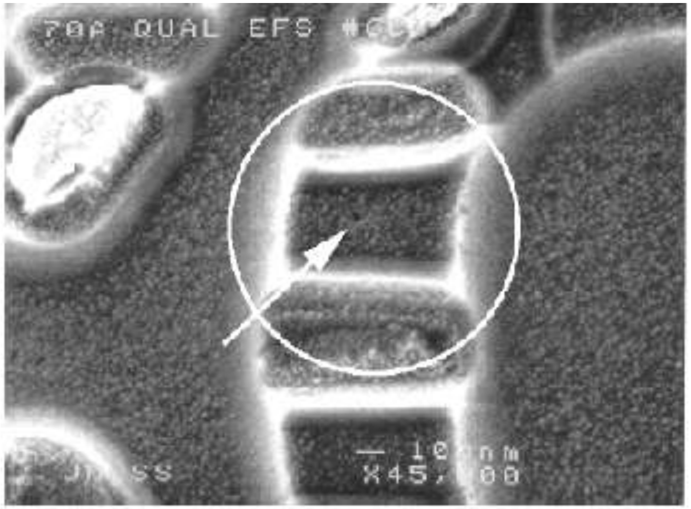


Source: "Hardware Security Requirements for Embedded Encryption Key Storage" Kilopass Inc. Whitepaper

Reverse Engineering CMOS NVM

Physical Inspection

- Antifuse effects may be made more visible through chemical enhancement
  - Similar to FA techniques used to identify oxide defects (i.e. pinholes)
  - Silicon selective etching will remove the polysilicon as well as expose where the silicon filament penetrated the gate oxide to create the leakage path

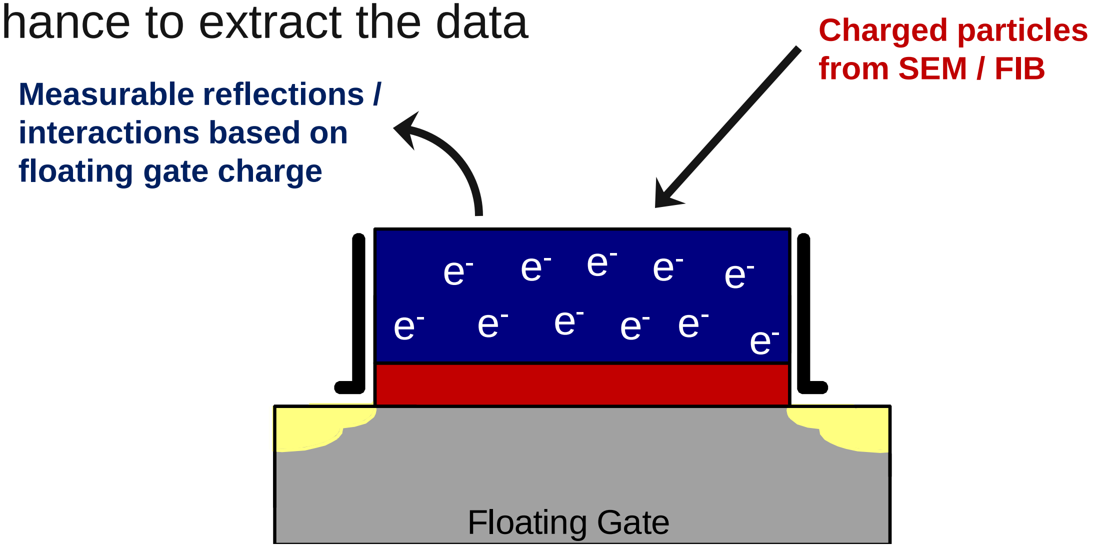


Source:
"Atomic Force Probe Analysis of Non-Visible Defects in Sub-100nm CMOS Technologies", Randal Mulder, Sam Subramian, Tony Chrastecky. Freescale Semiconductor, 32nd International Symposium on Testing and Failure Analysis

Reverse Engineering CMOS NVM

Electrical Inspection of Floating Gates

- Theoretically floating gate states can be identified with SEM or FIB based voltage contrast
  - Voltage and spatial resolution are within current technology limits
- The act of measuring disturbs the contents of the floating gate
  - Bombarding the floating gate with charged particles can change the state
  - Only 1 chance to extract the data



Charged particles from SEM / FIB

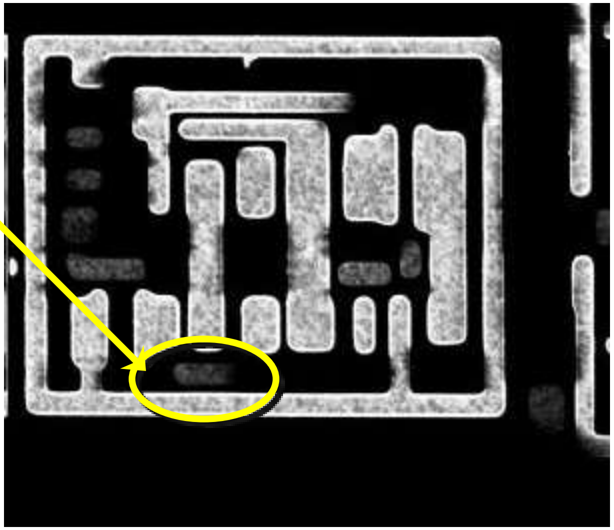
Measurable reflections / interactions based on floating gate charge

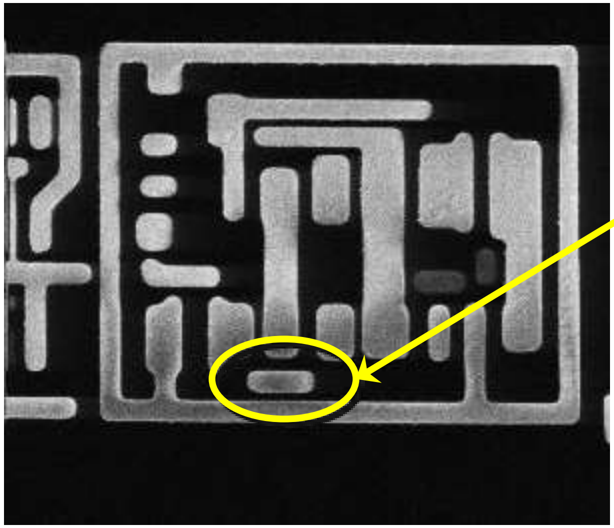
Reverse Engineering CMOS NVM

Electrical Inspection of Antifuse Technology

- Voltage contrast can be used to determine the contents of antifuse technology as well
  - Charge the polysilicon and track how quickly the charge leaks off to determine which cells are programmed (leaky) and which are not
- No disturb mechanism
  - Repeat the measurements as many times as needed to get the right settings

Dark spot – gate is in-tact





Bright spot – gate is leaking

Source:
“FIB Assisted Localisation and Preparation of Gate Oxide Fails”, Dr. Rüdiger Rosenkranz, Infineon Technologies

Conclusions

- Embedded NVM in standard CMOS processing is becoming mainstream for a variety of applications including security and encryption
  - Provides cost and process availability advantages over traditional mask-adder technologies
- Both floating gate and antifuse CMOS based NVM technologies are resistant to physical inspection based reverse engineering techniques
  - Antifuse based NVM can be made more visible through selective etch techniques
- Electrical inspection techniques are more effective on antifuse technologies than floating gates
  - Deprocessing and attempting to measure the contents of a floating gate NVM disturbs the memory contents
  - Antifuse technology is not disturbed by either deprocessing or electrical measurement techniques