CSCI 4974 / 6974
Hardware Reverse Engineering

Lecture 10: EEPROM/Flash

Nonvolatile writable memories

- Writable memory that persists after shutdown
- Typically much slower than RAM
- Often has endurance limitations

Types of NVRAM

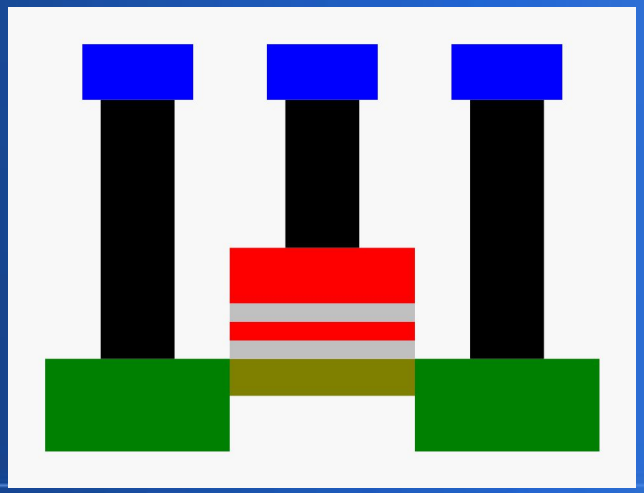
- Battery-backed SRAM
- EPROM
- EEPROM
- Flash (NAND / NOR)
- OTP (one-time programmable)
  - Soft OTP
  - Poly fuse
  - Antifuse

Battery backed SRAM

- Volatile memory + battery or supercap
- Data retention: until battery runs out
- Endurance: Unlimited
- Difficult to extract if not routed externally
  - May need to decap without removing power
  - Used in SecurID, FPGA boot key storage, etc
- Runs at normal logic voltages

Floating gates

- NMOS (typ.) transistor with two stacked gates
- Bottom floating gate isn't connected to anything
- Top control gate is connected to WL
- CG low? Transistor is off like normal
- CG high? Voltage on FG determines state



Floating gate NVRAM

- Several different structures possible
- All are basically NAND or NOR like ROM
  - Addressing and array layout is identical to ROM
  - Read behavior is identical to ROM
- But the transistors are programmable now!
  - Charge on FG = transistor on = read “0”
  - No charge on FG = transistor off = read “1”
- Oxide breakdown/trapped charge limits lifetime

Reading floating gate NVRAM

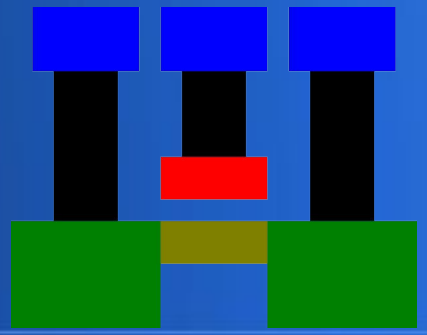
- Drop probes down on bus and sniff
- Polish off upper layers, read charge with SCM
- Use built-in readback function
  - May require defeating read protection

Multi-level cells

- Store 4 (or 8) discrete levels of charge on FG
- Allows storage of 2 or 3 bits per cell
  - Much higher density than SLC (single-level cell)
- But worse noise margins
  - 1/4 or 1/8 the leakage is enough to flip bits

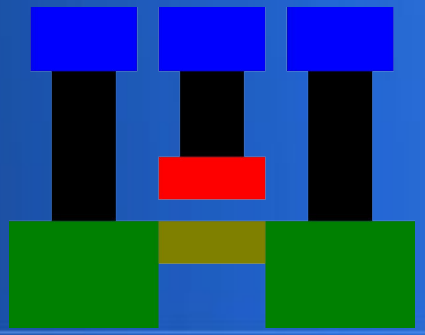
Fowler-Nordheim tunneling

- In the presence of a strong electric field (~1V/nm), electrons can “jump” through an insulator (including vacuum)
- This is the same effect responsible for the operation of a field emission electron gun!
- We can use this to move electrons on/off the floating gate.



Channel hot electron injection

- Alternative method of jumping tunnel oxide
- Apply HV from source to drain
  - Creates high-speed electron beam in channel
- Apply HV to control gate
  - Deflects e-beam up through oxide and into FG
- Requires more current than F-N
  - but faster
- Only works for NOR structures



UV ionization

- SiO_2 ionizes slightly under short-wave UV
- Becomes weakly conductive
- Can bleed charge off FG

EPROM

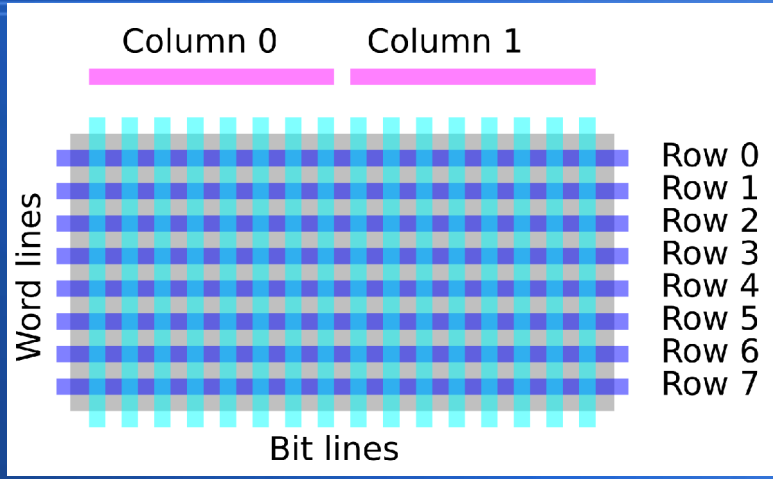
- Eraseable Programmable ROM
- Data retention: 10 years
- Endurance: 100 - 1000 erase cycles
- Requires HV for program (CHE), UV for erase
- Always SLC

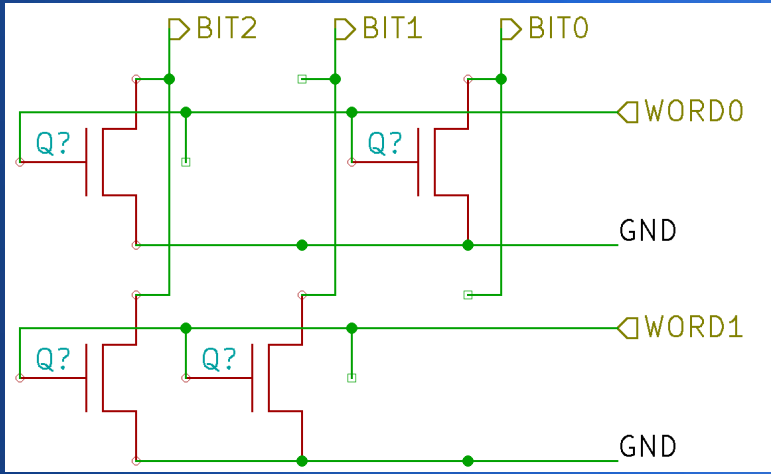
EPROM operation

- Erase (discharge all FGs, set all bits to 1)
  - Apply UV radiation and let FGs drain
  - Takes ~30 mins

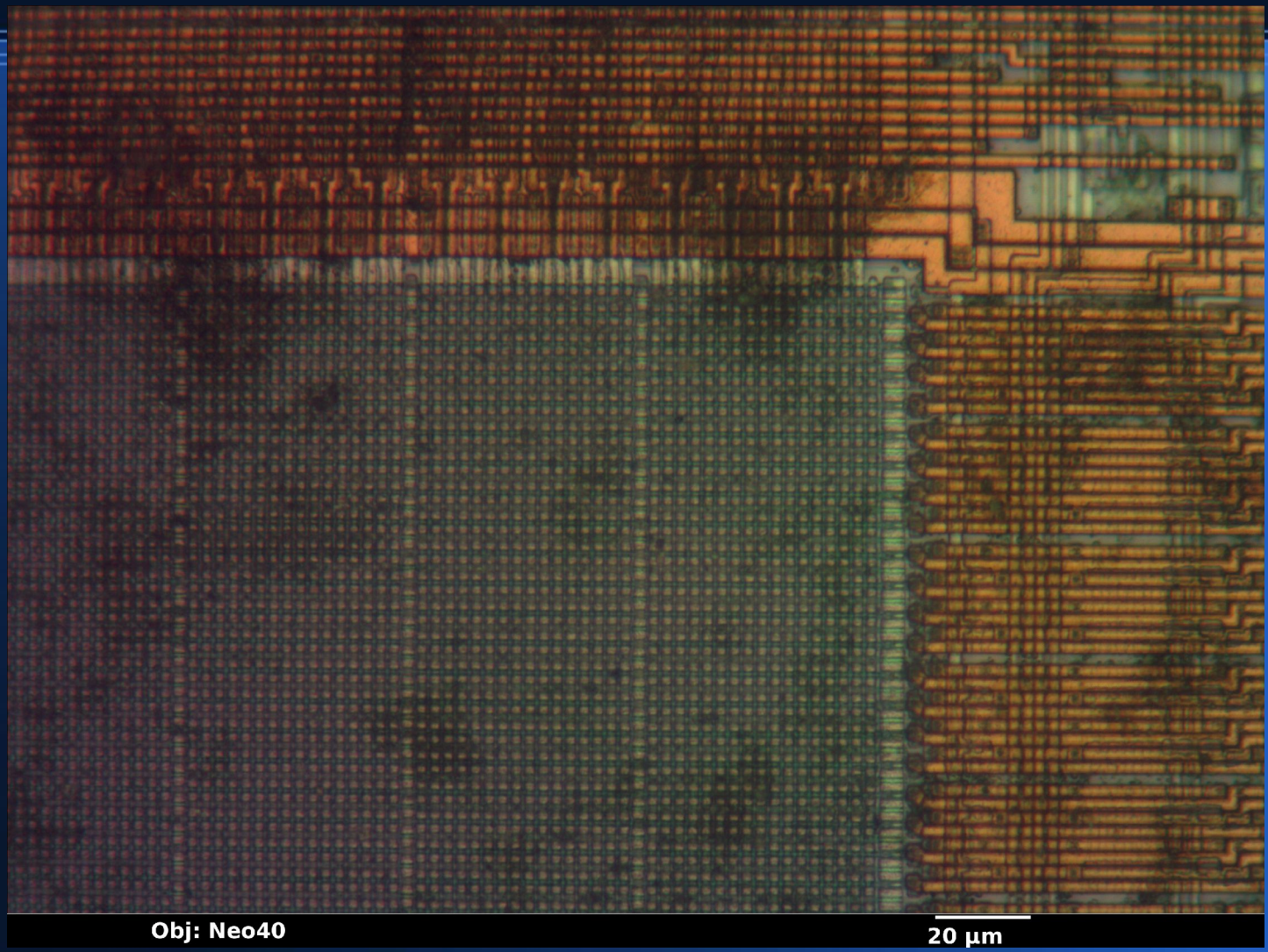
EPROM operation

- Program (set bits to 0)
  - Apply HV to WL
  - Apply HV to BL
  - Leave other BLs at 0V





EPROM from PIC12CE518



Recognition

- Usually found in older processes (500+ nm)
- External Vpp required to program device
  - Does not have HV generator on die
    (no point - need UV to erase anyway)
- UV window is a near-100% indicator of EPROM
  - But non-windowed (OTP) EPROMs exist too
- Can be tricky to distinguish from implant ROM
  - Both are 1T cells without HV generators nearby

EEPROM

- Electrically eraseable PROM
- Data retention: up to 100 years
- Endurance: up to 1M erase cycles
- F-N tunneling for program/erase
- NOR structure with 2 transistors per bit
  - Select transistor in series with FG transistor
- Always SLC

EEPROM operation

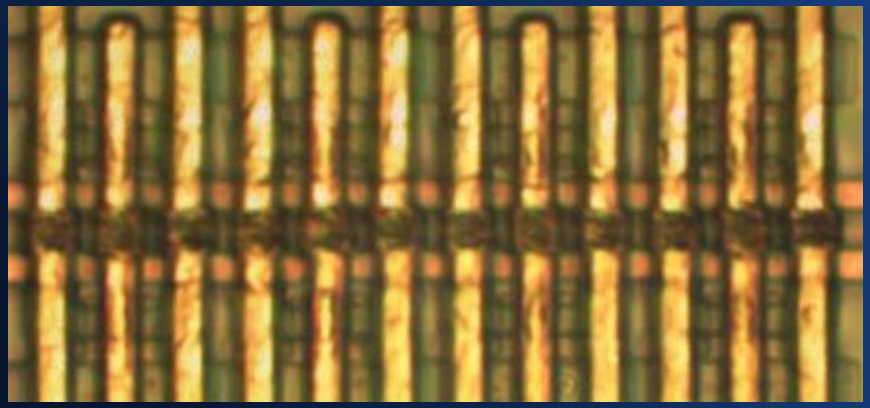
- Erase
  - Turn on select transistor but pull BL low
    - Both ends of storage channel are at 0V
  - Apply HV to control gate of FG transistor
  - Electrons tunnel from channel to FG
- This seems to be inverted polarity vs most other FG memories, but most published designs seem to work this way!
  - http://people.rit.edu/lffeee/EEPROM.pdf

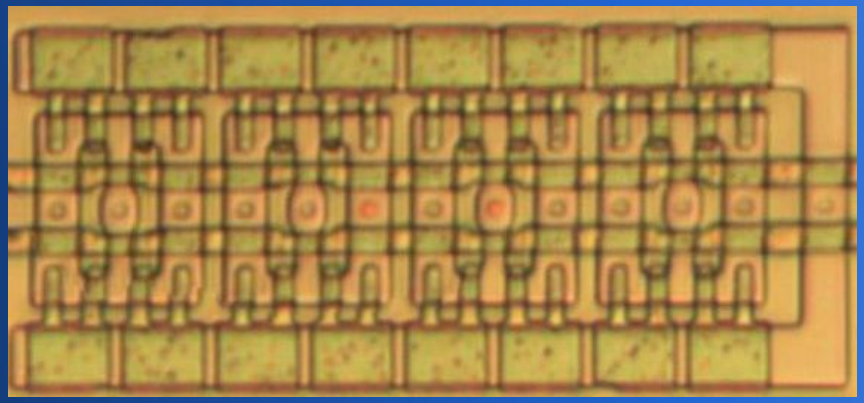
EEPROM operation

- Program
  - Turn on select transistor
  - Apply HV to BL
  - Pull control gate to ground
    - FG transistor is turned off (no CHE flow)
  - Electrons on FG tunnel off into channel

EEPROM from ST 24C02

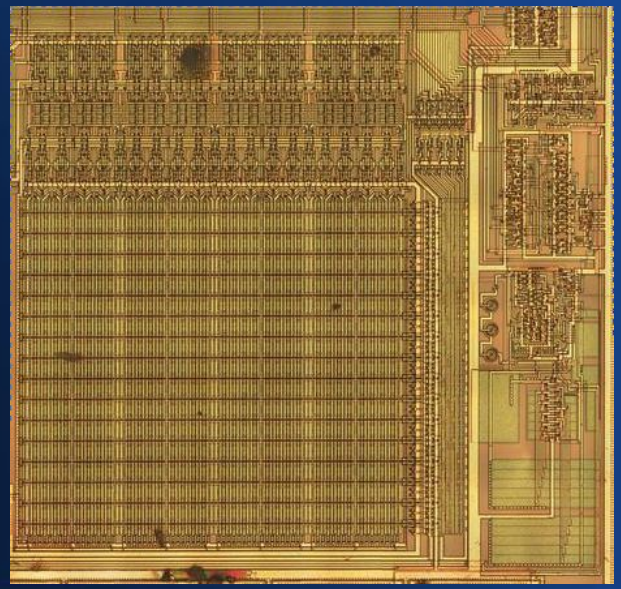
- Green squares are FGs
  - One finger for tunnel oxide
  - One finger for transistor
- Four cells per square, 16 cells in image





Recognition

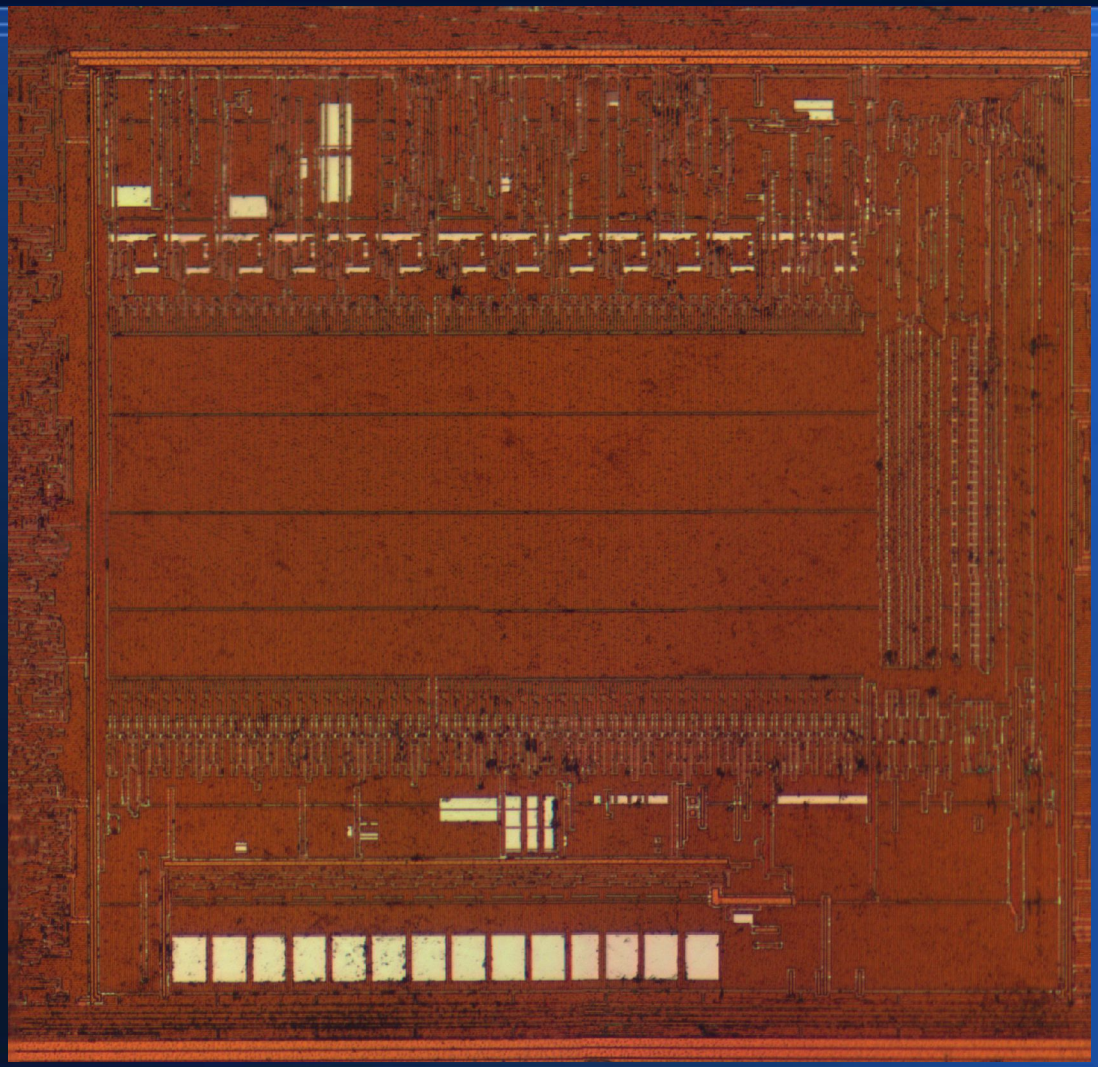
- Larger cells (2T)
- On-die charge pumps for program/erase
  - Look for big capacitors near memory array



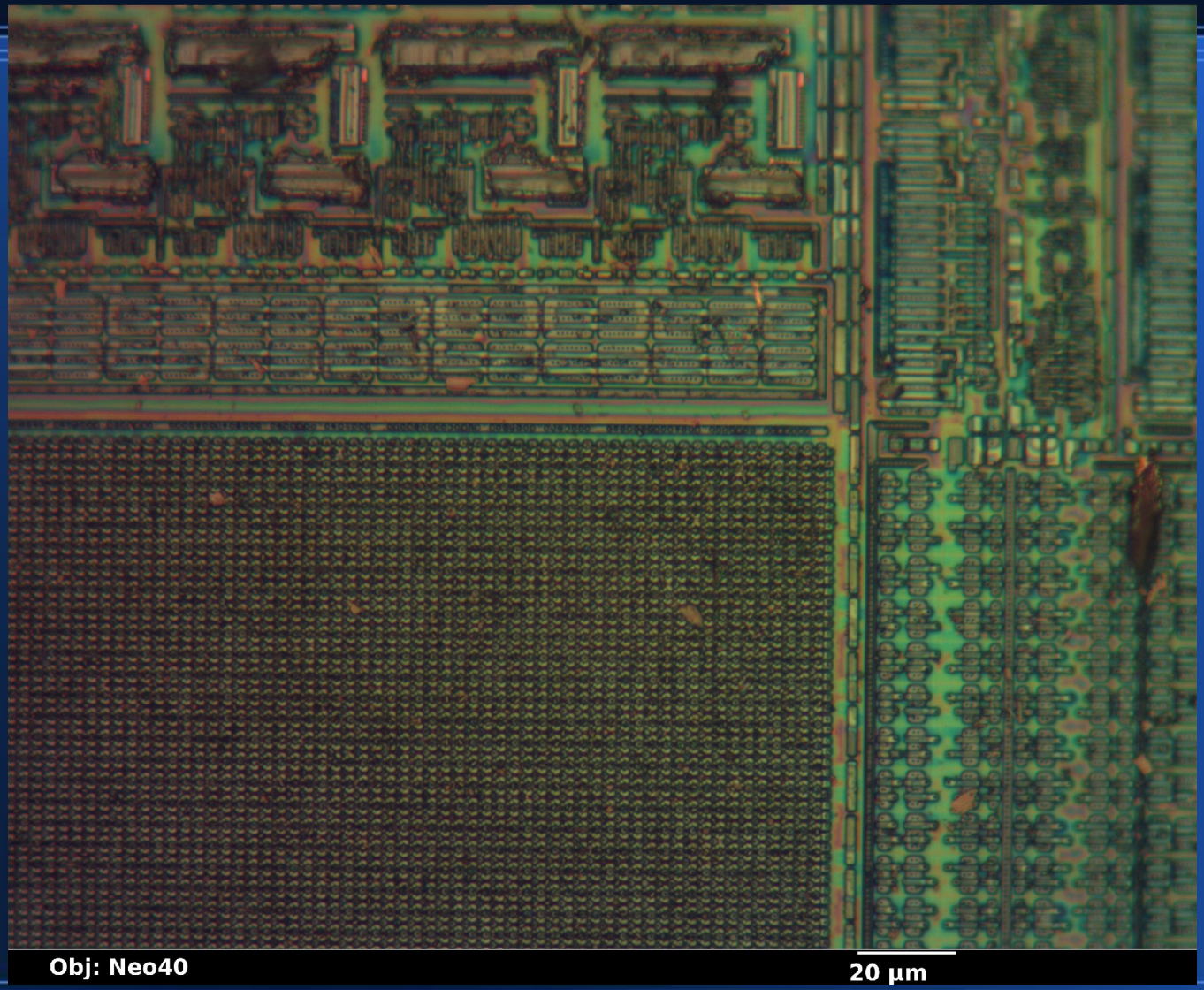
NOR flash

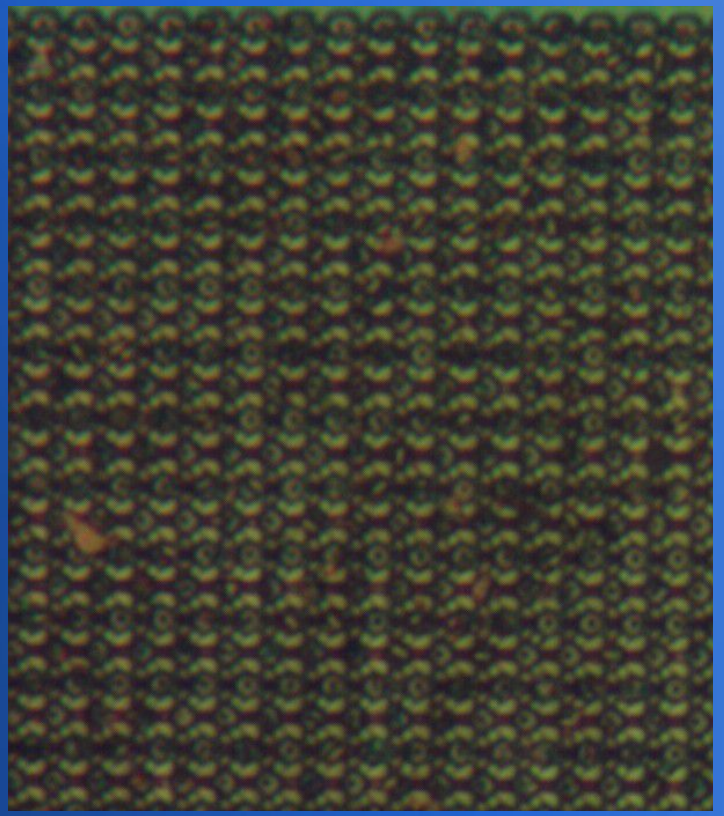
- Data retention: 20 years or more
- Endurance: 100K cycles typical
- CHE for program, FN for erase
- Always SLC
- Small (1T) cells
- Typically larger processes with high yields
- Commonly used for firmware storage

NOR flash (PIC12F683)



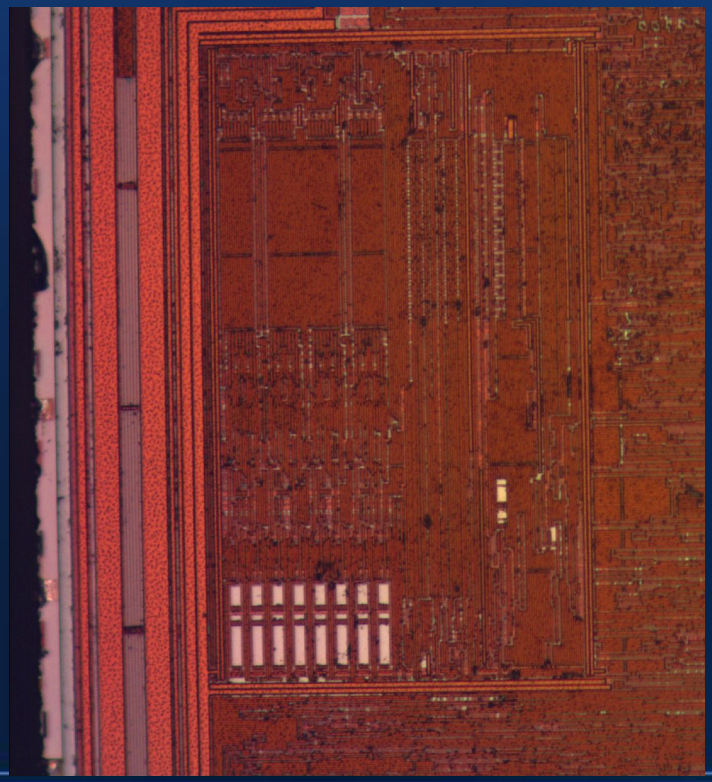
NOR flash (PIC12F683)

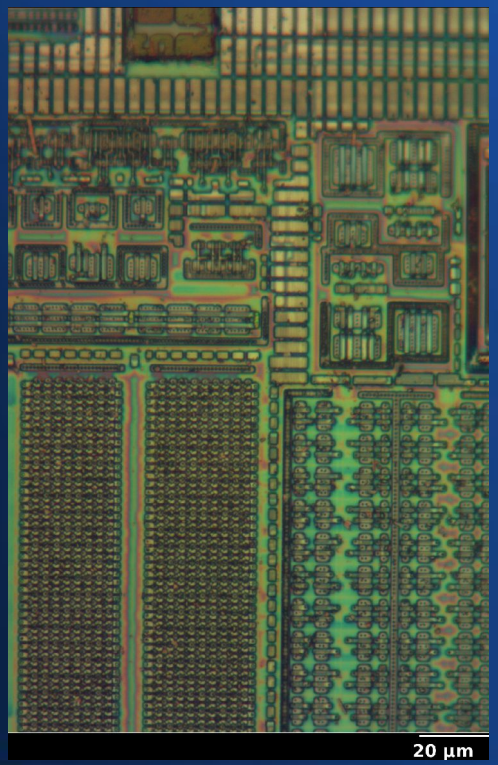


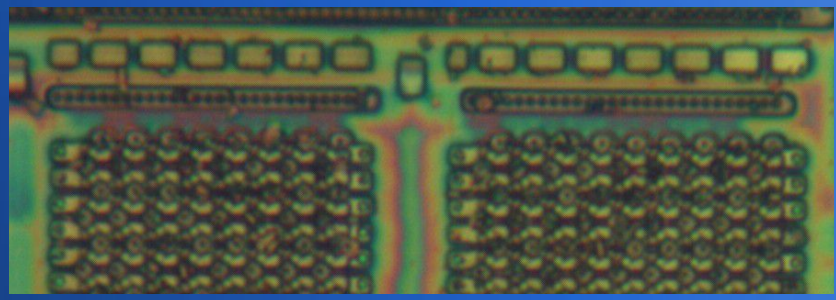


NOR “EEPROM” (PIC12F683)

- Datasheet calls it EEPROM but cell structure looks like NOR flash with 8-bit pages







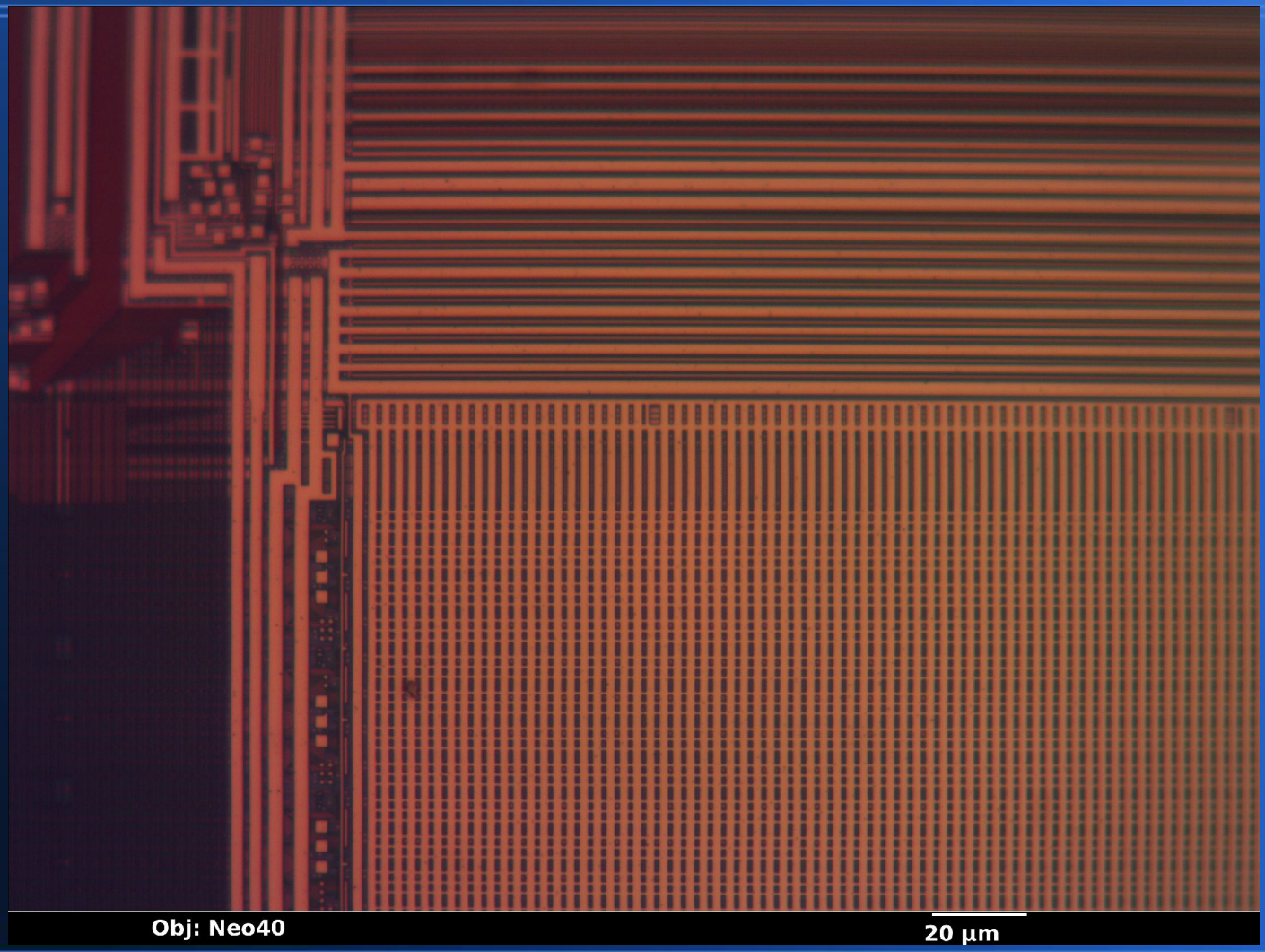
Recognition

- Smaller cells (1T)
- On-die charge pumps for program/erase
  - Look for big capacitors near memory array
- Most MCU firmware storage is NOR flash

NAND flash

- Data retention: 10 years
- Endurance: ~100K cycles SLC, ~10k MLC
- FN for program/erase
- Small (1T) cells
- Typically leading-edge process with poor yields
  - Lots of bad bits, ECC is mandatory
- Used for bulk data storage, typically not byte-addressable

NAND flash (random SD card)



Recognition

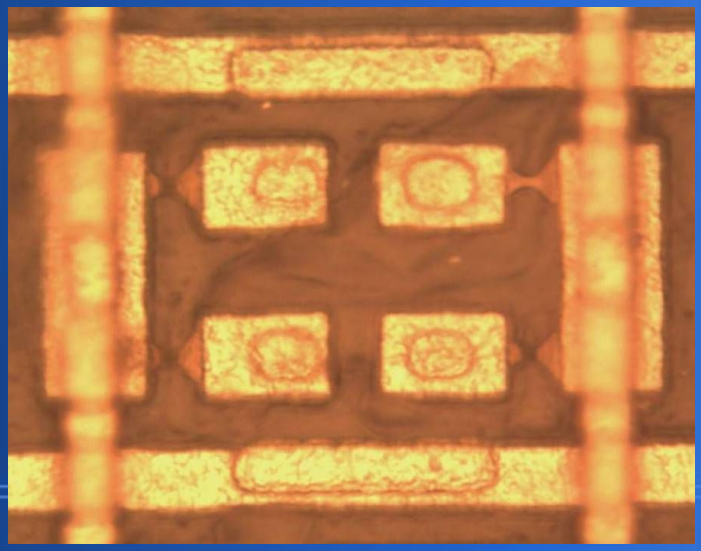
- Smaller cells (1T)
- Very dense layout due to less ground lines
- On-die charge pumps for program/erase
  - Look for big capacitors near memory array
- Almost never seen inside larger chips, usually standalone bulk data storage

OTP memories

- One-Time Programmable
- Soft OTP - physically eraseable, but no interface provided. EPROM w/o window, flash w/o erase circuit (or gated part of array)
- Fuse - conductor breaks when programmed
- Antifuse - insulator shorts when programmed

Fuse memory

- Each cell is a short length of polysilicon/metal
- Apply high current to blow out fuse during programming
- Horizontal layout, optically readable
- Data retention: Unlimited
- Endurance: One cycle
- NatSemi DMPAL16R



Recognition

- Fuse links are visibly necked-down to provide rupture points
- In a non-blank device, some will be blown
- Fuses may be on either a poly or metal layer

Laser fuse memory

- Similar to electrically programmed fuses
- Can be denser, no Vpp needed on chip
- Blow out fuse links with laser before packaging
- Must be programmed before die is packaged
- Used for unique serial #s etc

Recognition

- Looks a lot like electrical fuse memory
- Fuse links need to be reachable by laser
  - Can't be covered by filler or upper metal layers
- Programmed bits have cut marks around them
  - Shows up nicely in darkfield optical or SEM

Antifuse memory

- Similar to fuses, but backwards
- Burn through insulating material with HV
- Link becomes conductive
- Tends to be vertical (inside via), hard to read
- Actel FPGAs

Recognition

- Vertical layout (inside vias)
- In FPGAs etc, may live inside interconnect
  - Hard to find, looks just like a via at first
- Can be used for bulk memories too
  - Laid out much like via ROM
  - but field programmable

Questions?

- TA: Andrew Zonenberg <azonenberg@drawersteak.com>
- Image credit: Some images CC-BY from:
  - John McMaster <JohnDMcMaster@gmail.com>