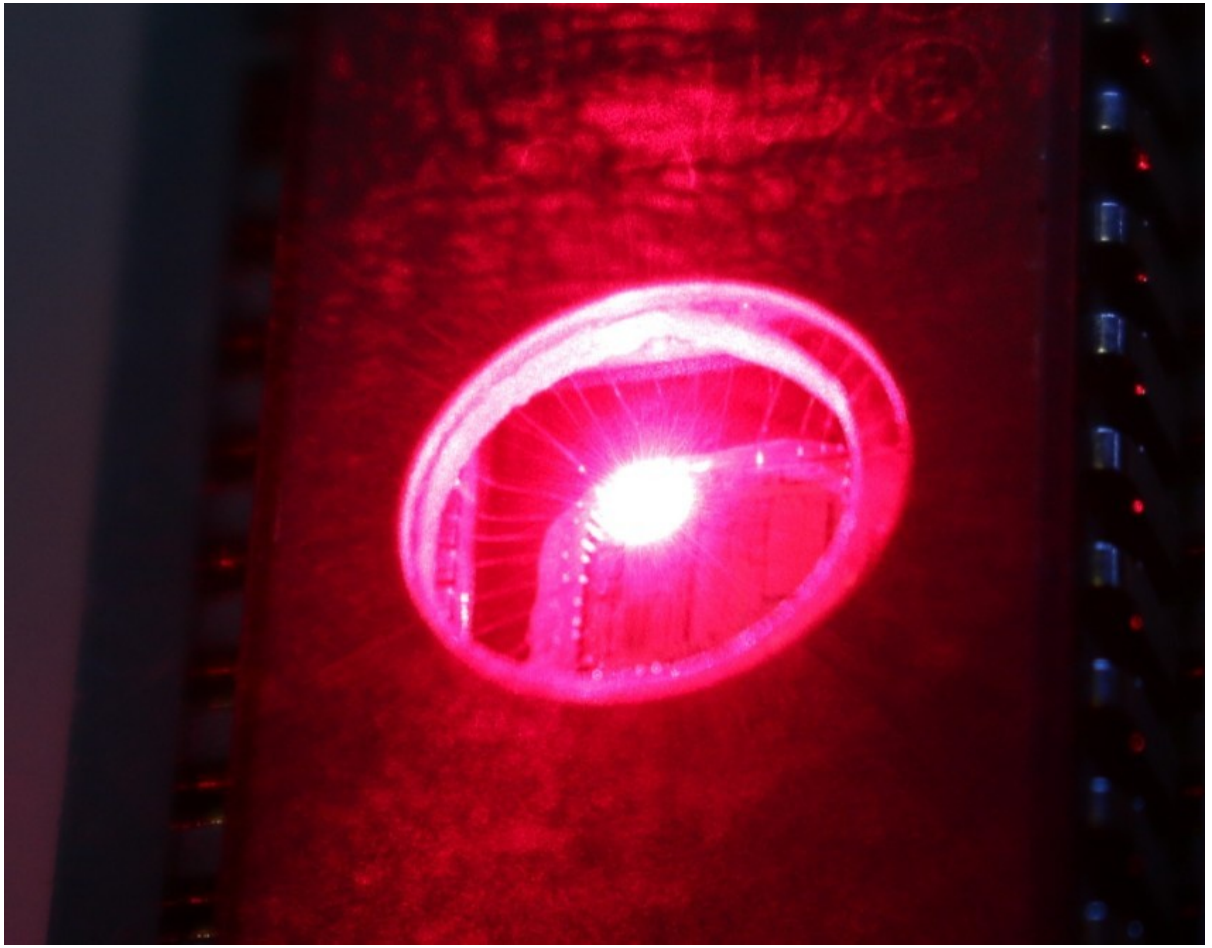
Silicon photonics



John McMaster
JohnDMcMaster@gmail.com

What

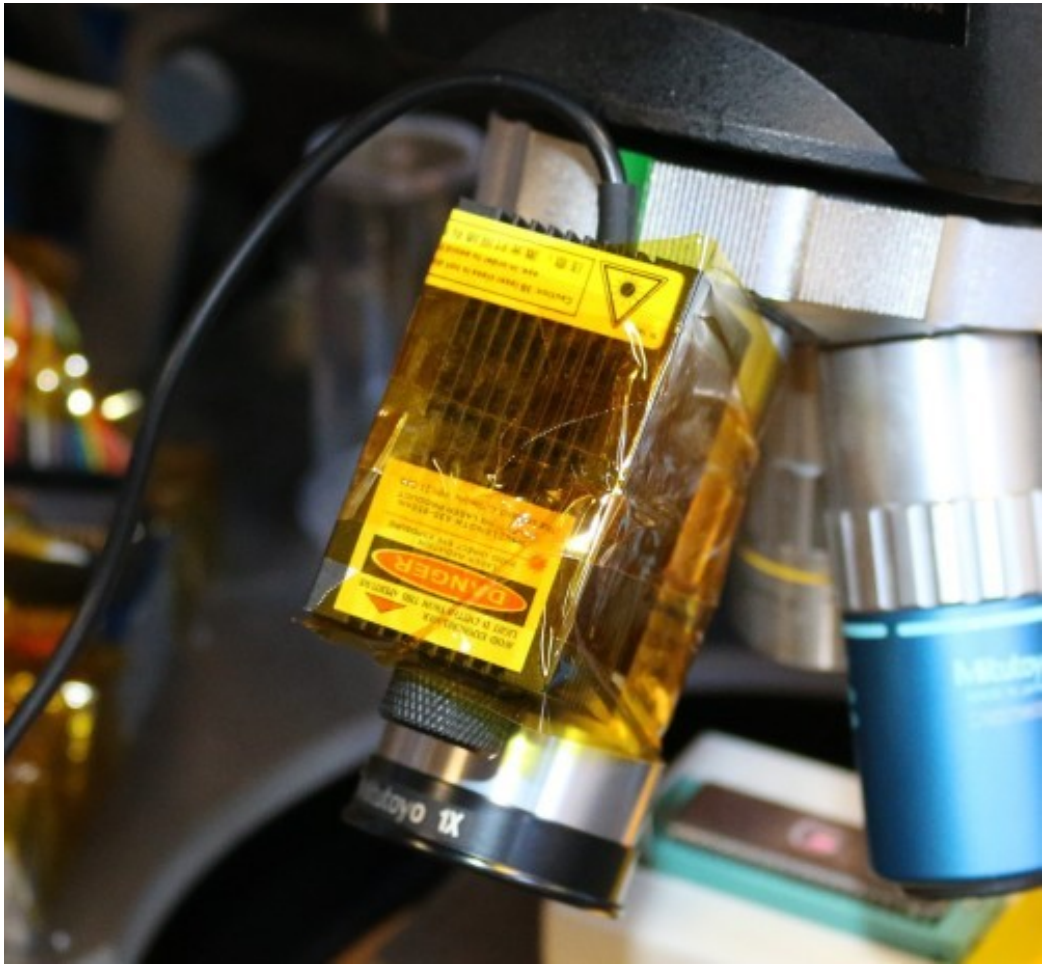
- Explore visible light effects on silicon
- Photon strikes material to generate charge
- Any photon will do: optical, x-ray, etc
- Effects
  - Increase leakage
  - Turn on transistor
  - Flip bits
  - Read out bits

Project goals

- Disable code protection
  - For research purposes only of course
- Read encryption keys
- Enhance DPA: unbalance protection

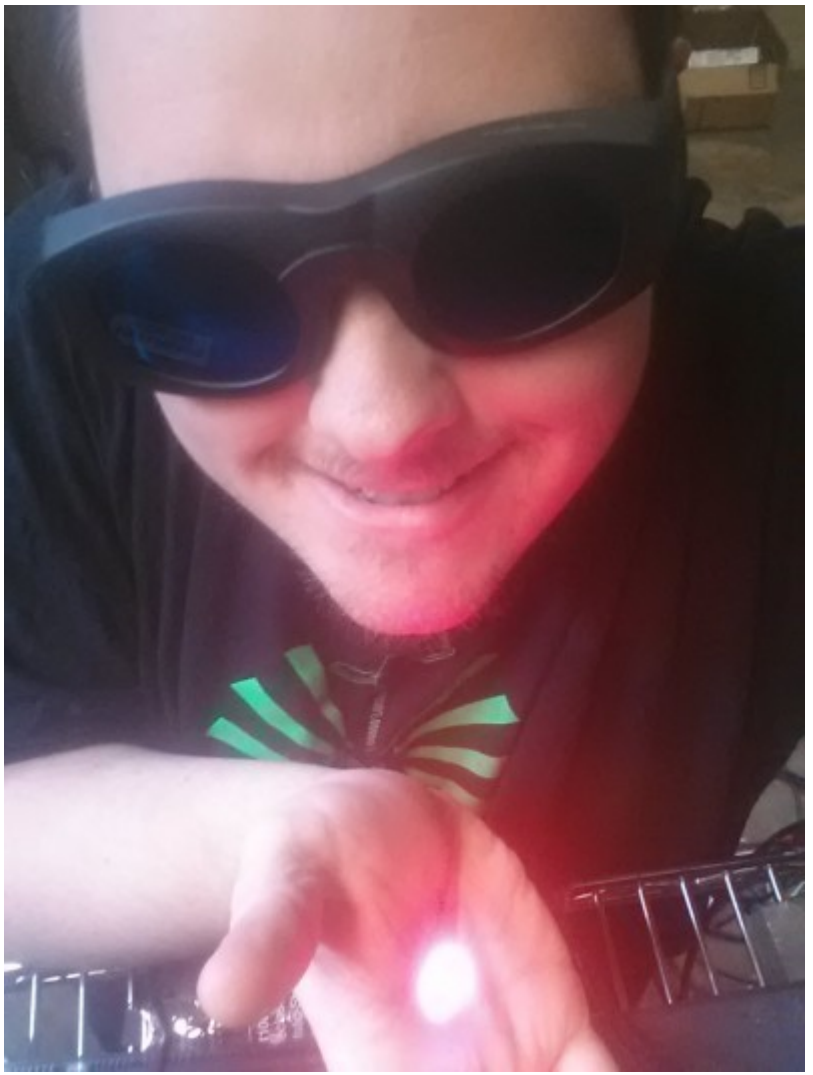
Video: IC cell phone demo

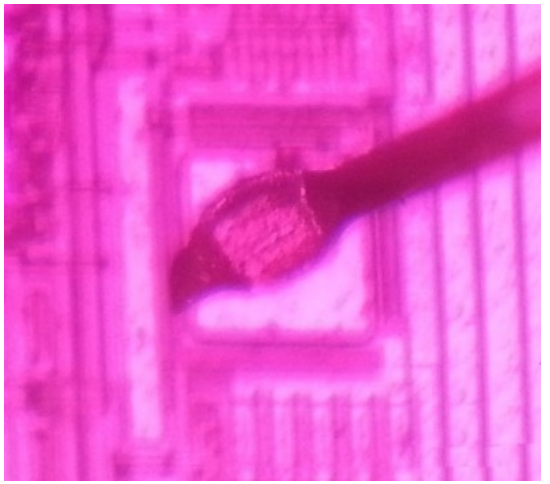
The stage: ezlaze Nd:YAG + 200 mW red



- So I can lase while I lase

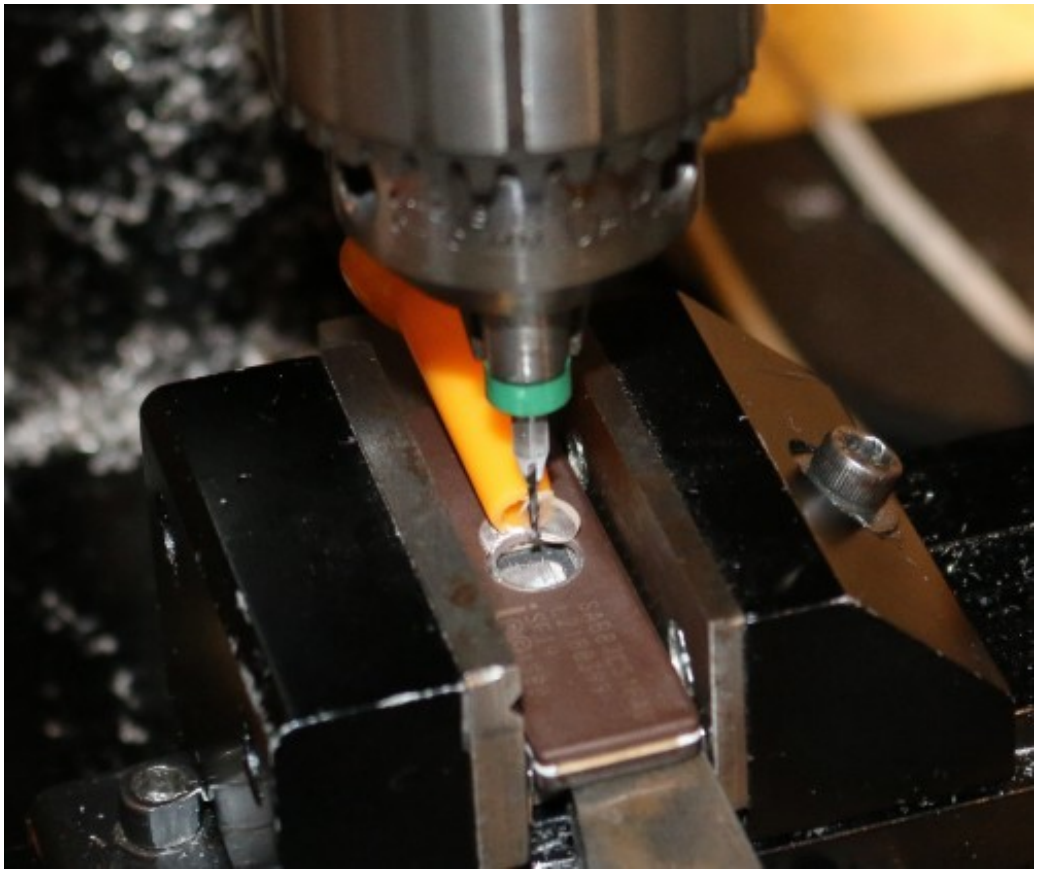
Safety third

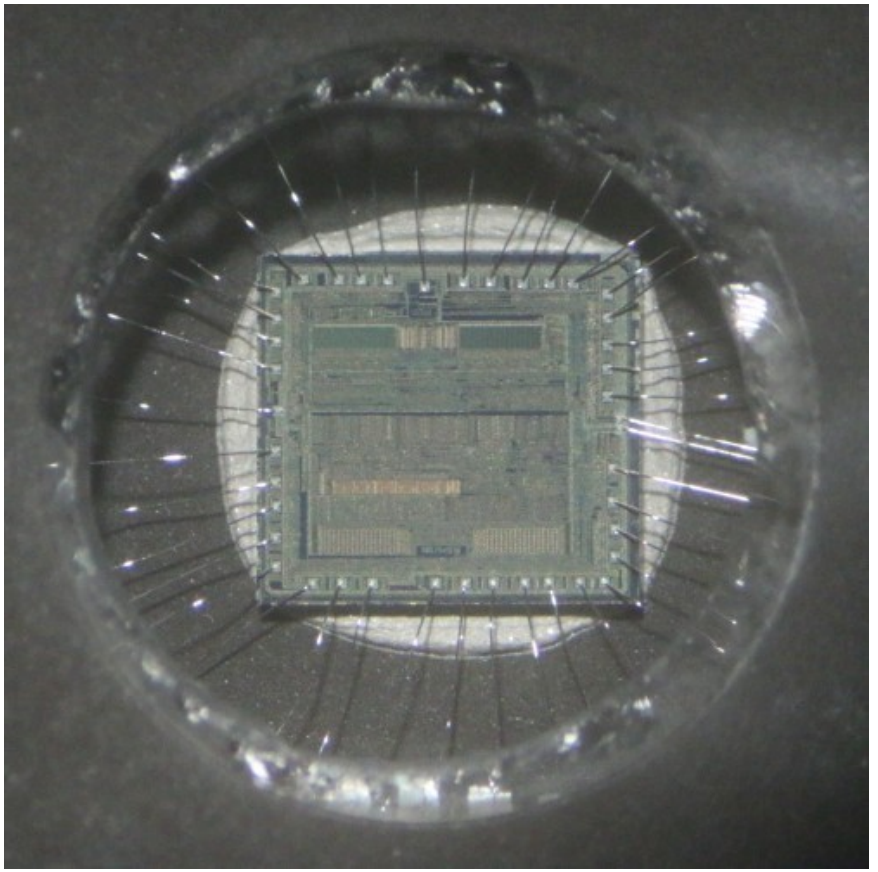


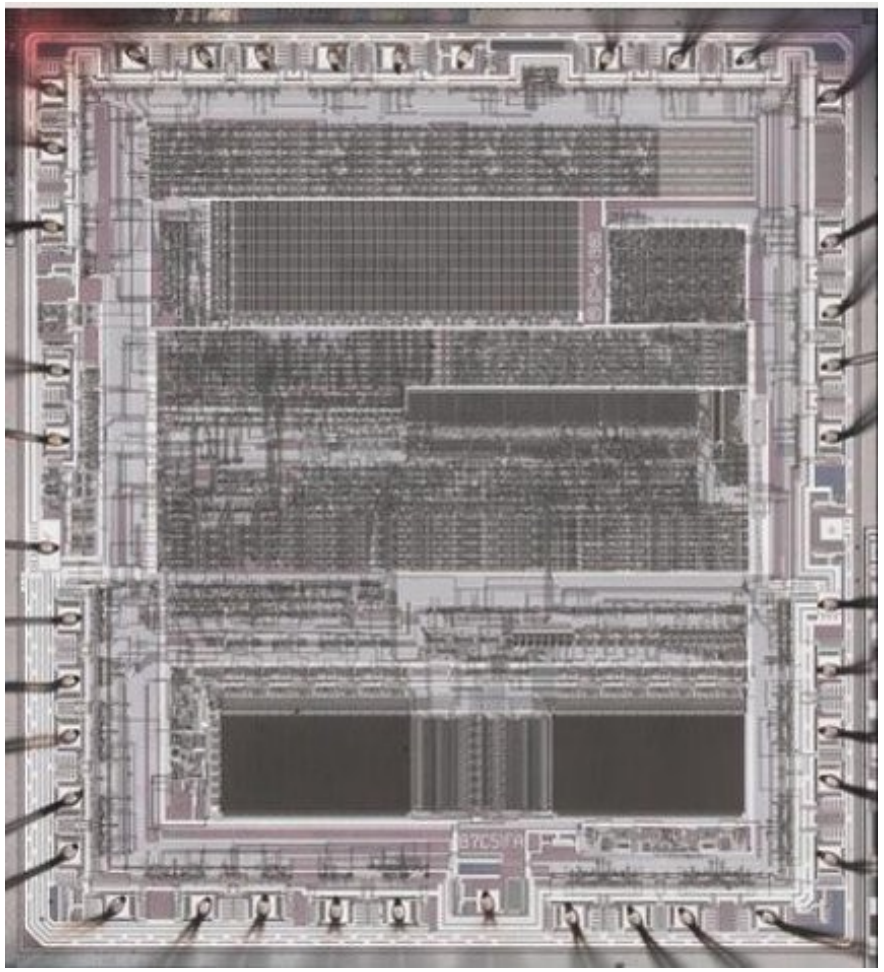


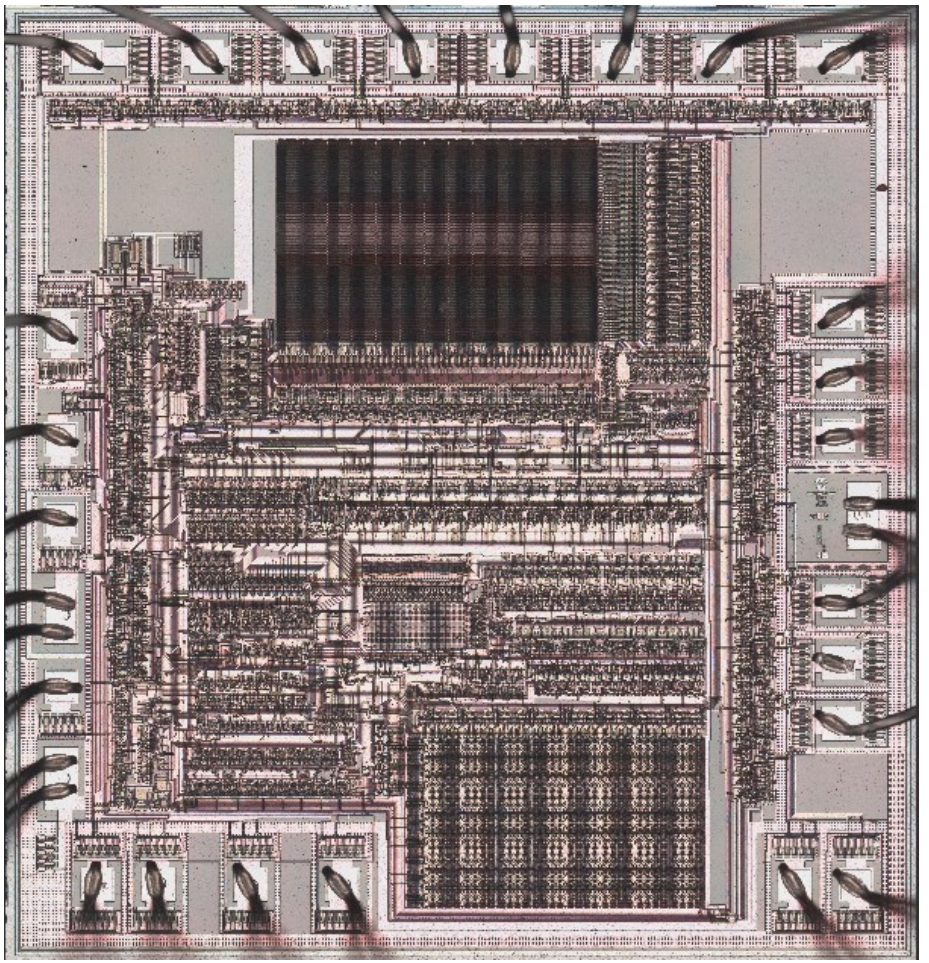
Removing window

- Fix beam distortion





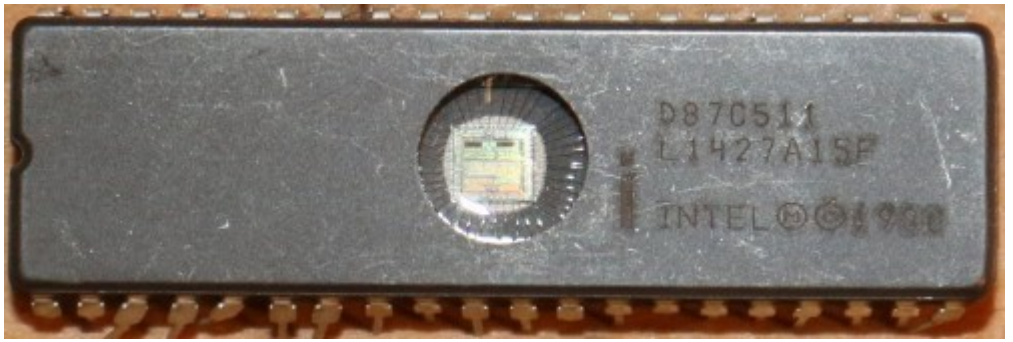


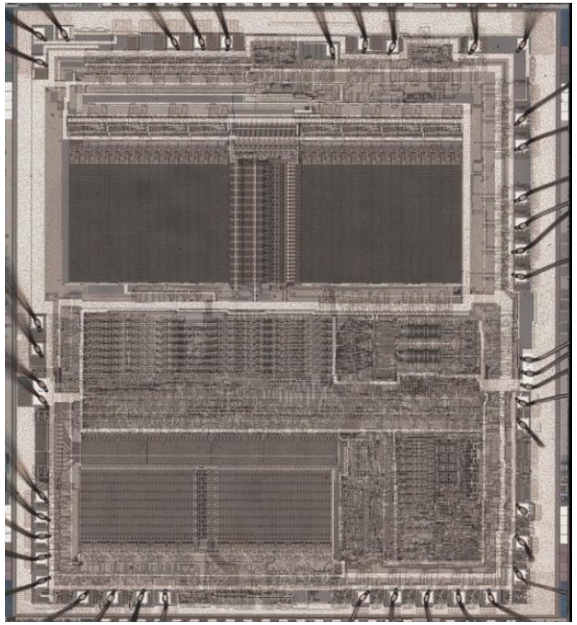


Targets

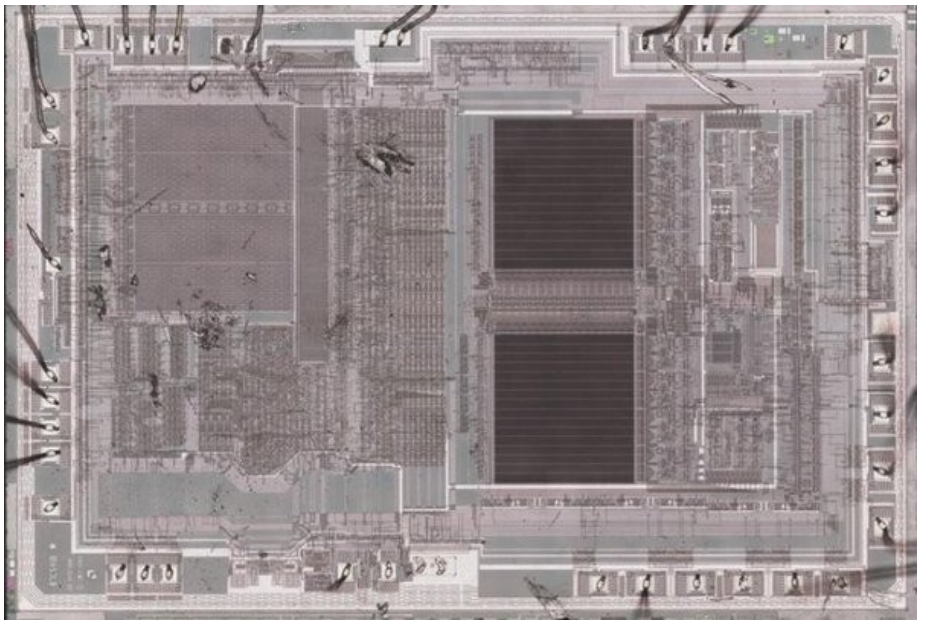
The players: 8751 family

- Early secure MCUs
- ~1980
- EPROM or OTP (rarer)
- Secure MCS 51
  - Code protect
  - XNOR encryption table

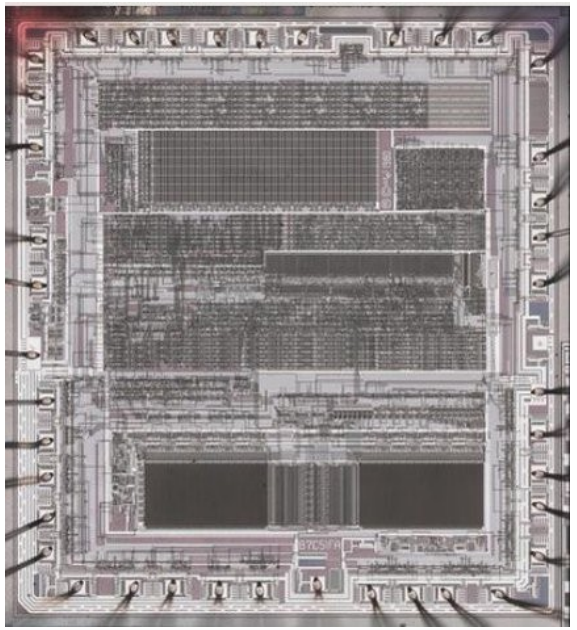




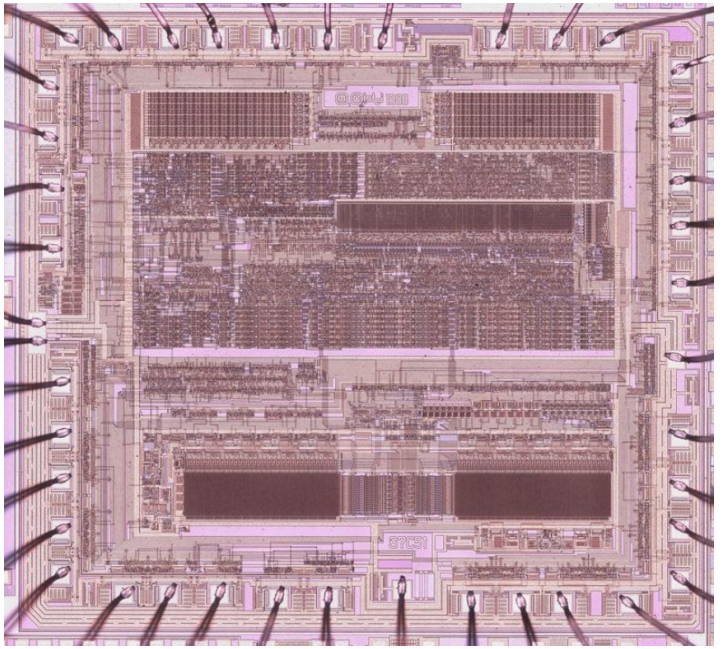
8751H



87C541B



87C51FA

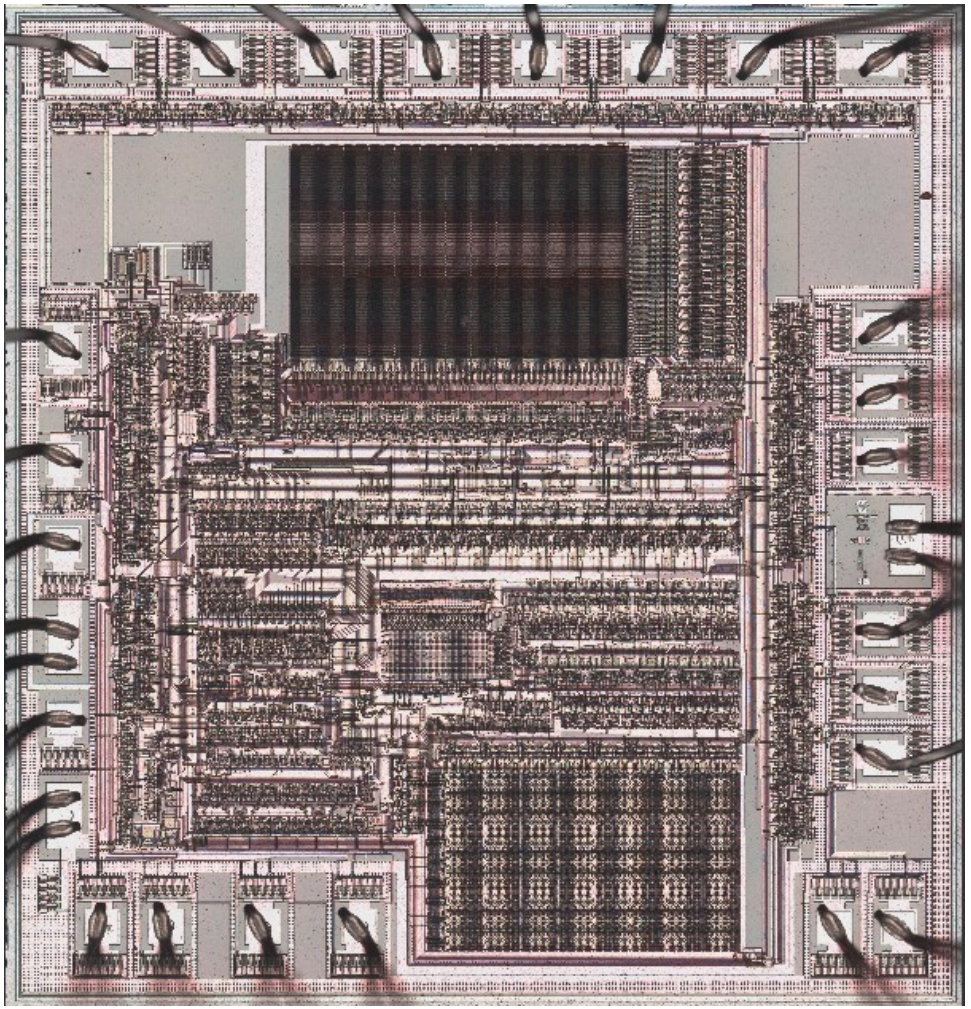


87C51I

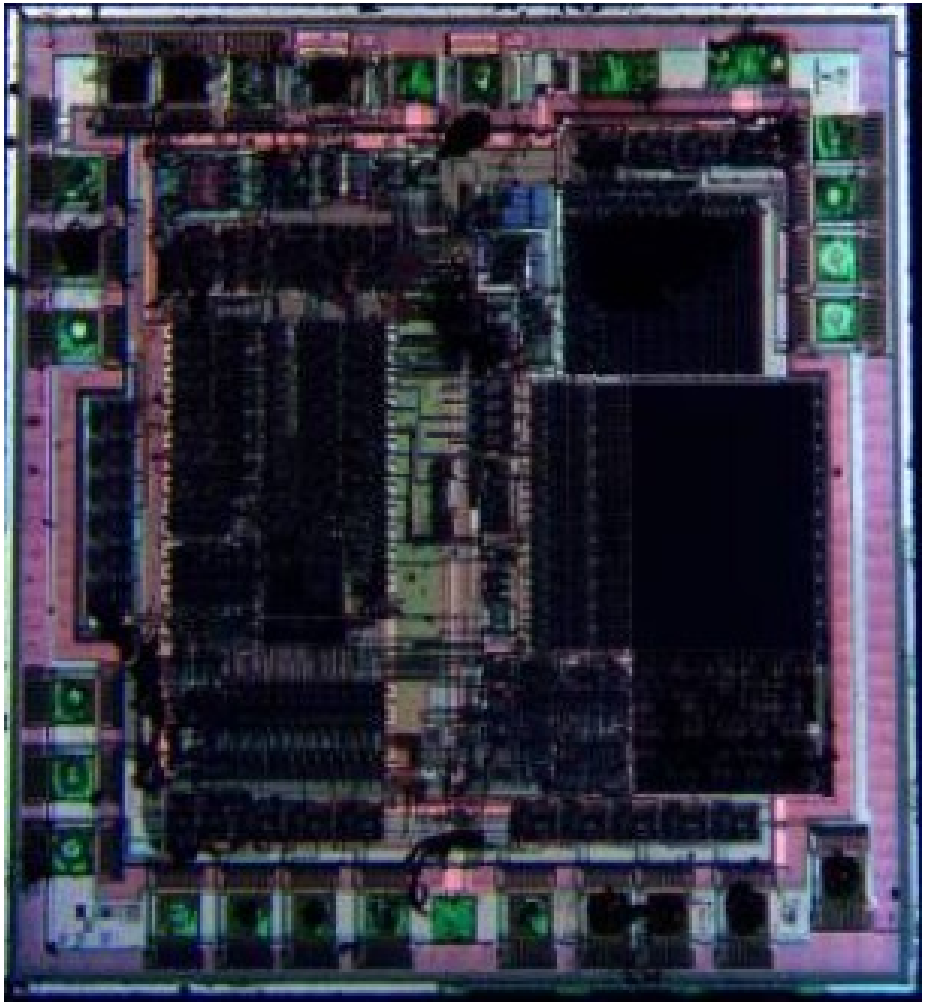
The players: PIC16C57

- ~1990
- EPROM or OTP
- “Secure” PIC16C5X
  - Protect => XOR 3 nibbles
  - Address limit?
- PIC16C57C known fuse location

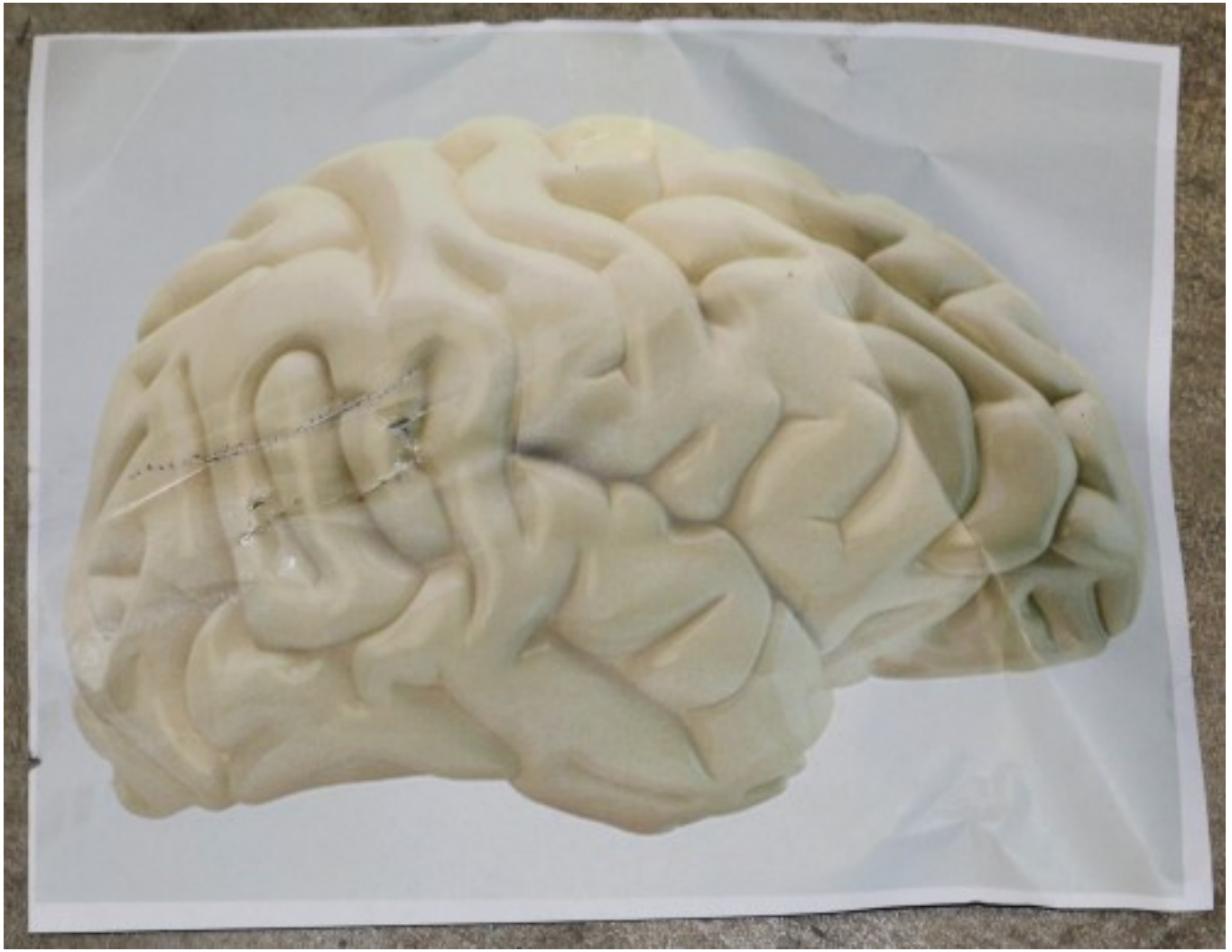
This isn't the PIC16C57 you're looking for



PIC16C57



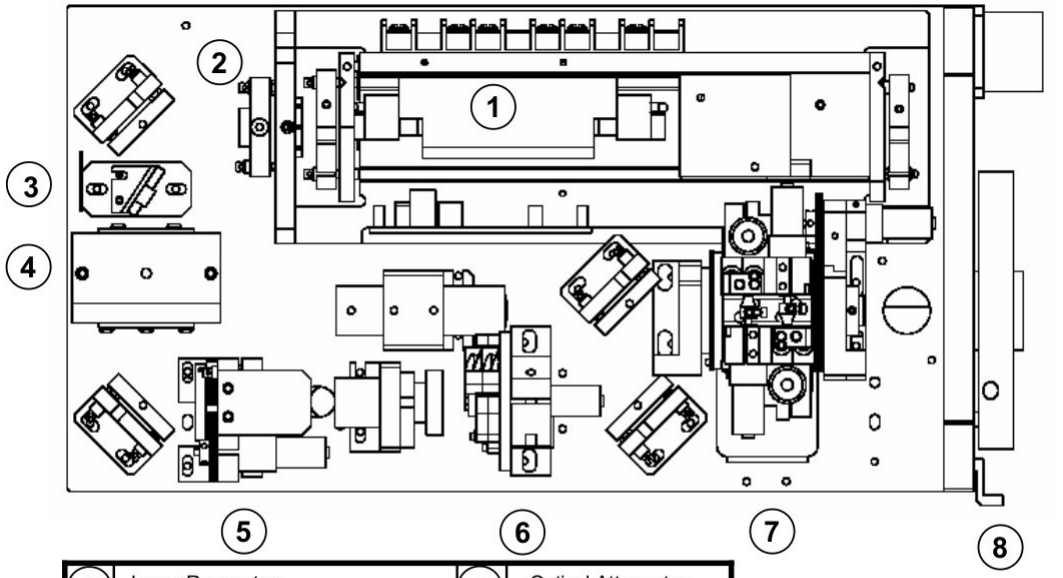
PIC16C57C



Brainscope / Nd:YAG fuzzing

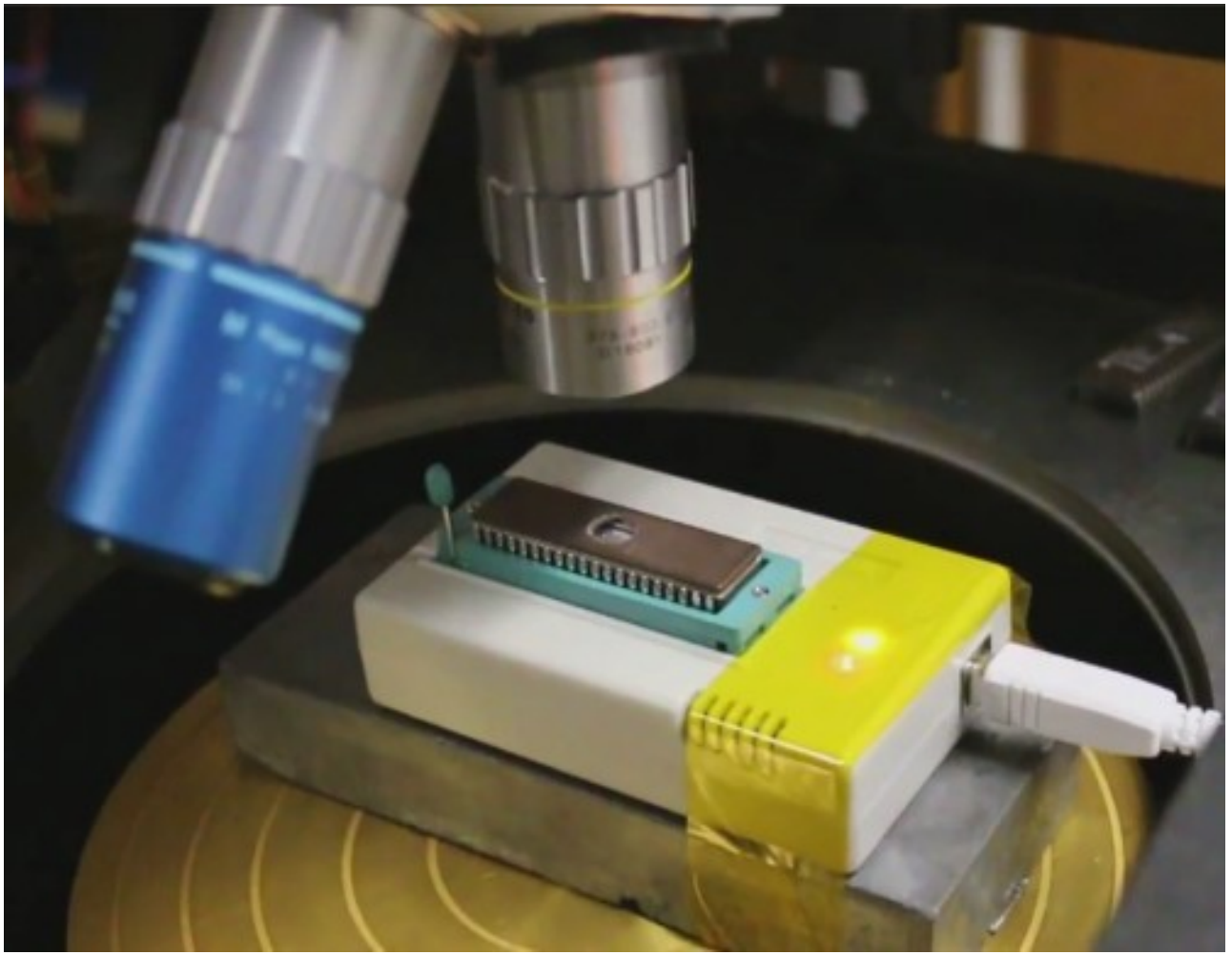
Brainscope Nd:YAG

- High power pulse: cut traces => kill IC
- 532 nm, 355 nm Nd:YAG laser
- Computer control



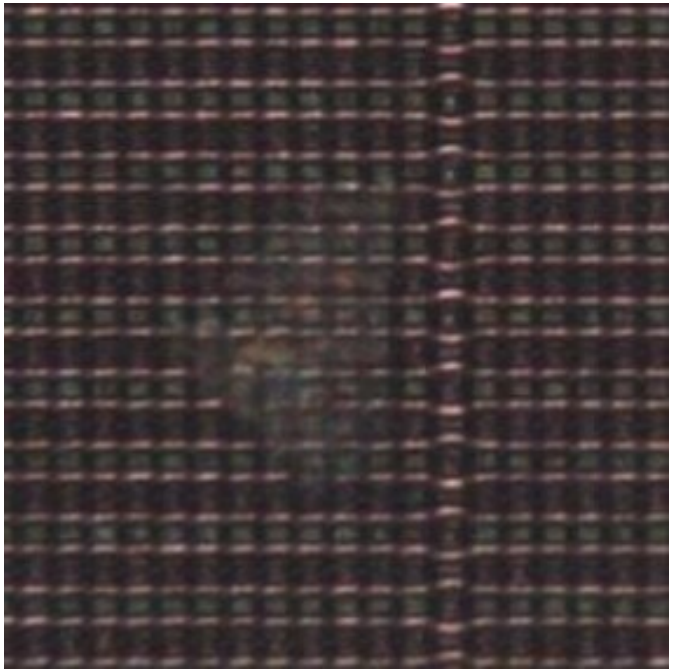
1	Laser Resonator	5	Optical Attenuator
2	Second Harmonic Generator (SHG)	6	Wavelength Selector
3	Polarizer	7	XY Shutter
4	Third Harmonic Generator (THG)	8	Safety Shutter

Video: brainscope fuzzing



87C51 Nd:YAG: erase fuses

- EPROM erases < 400 nm => 355 nm erases
- Overnight barrage: nothing erased
- UVA lamp: nothing erased

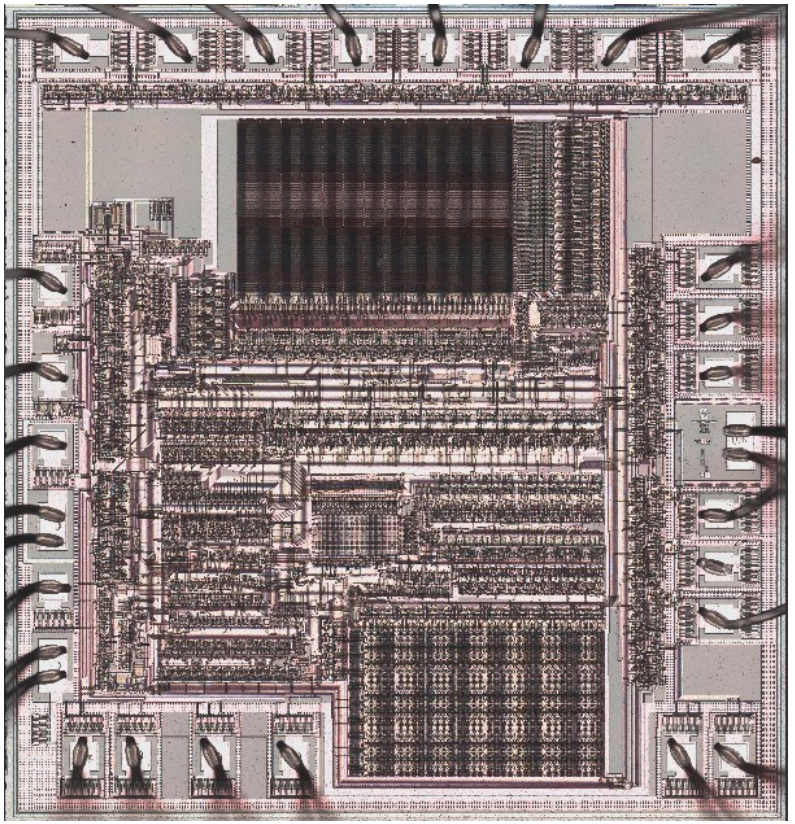


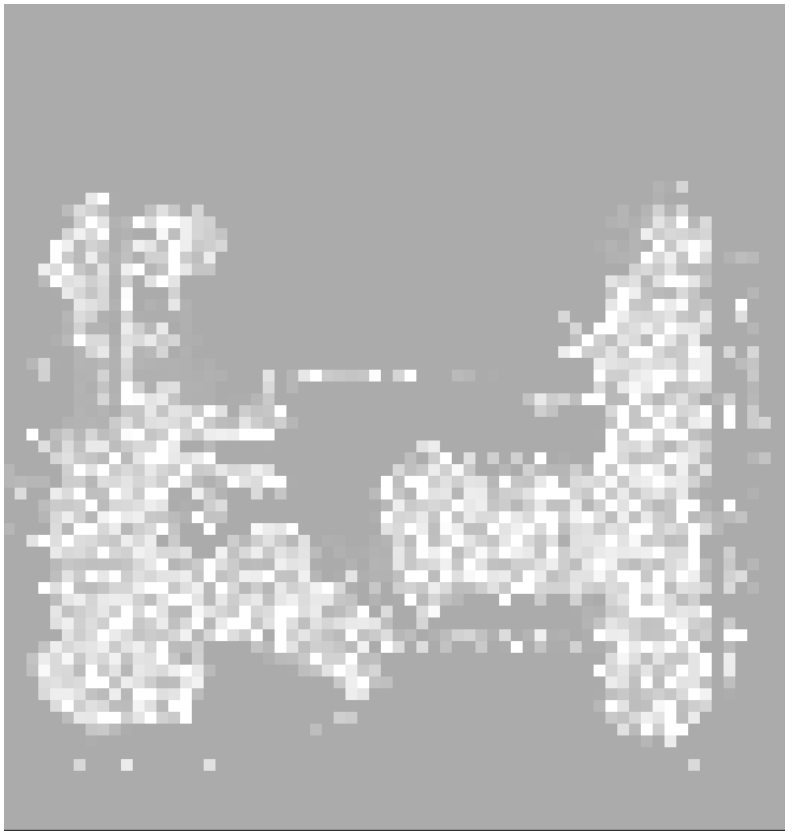
87C51 Nd:YAG

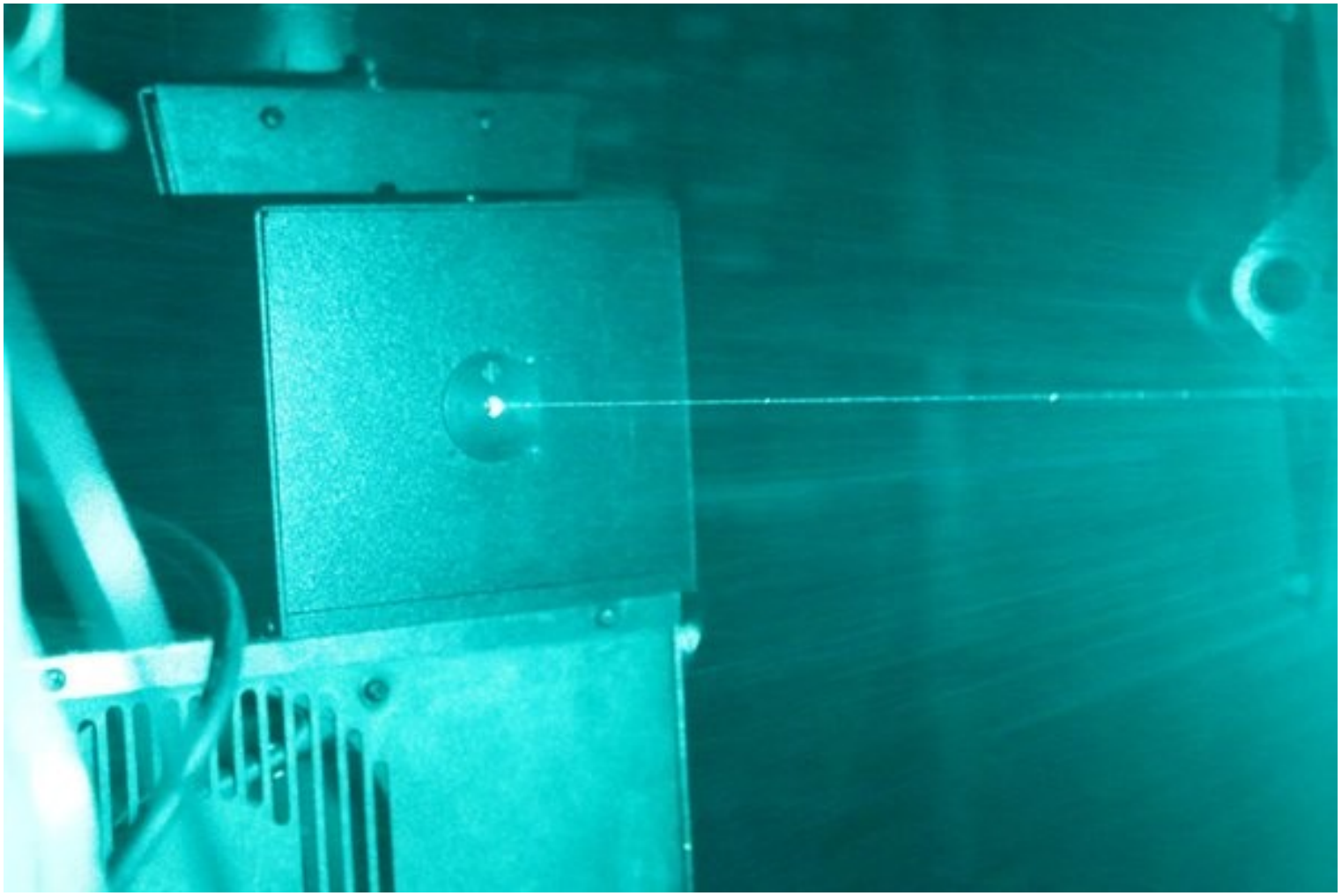
- Some areas more active than other
- Need to sweep beam size
- No breakthroughs
- Try 8751

PIC16C57 Nd:YAG

- Very sensitive: easy to force pad values
- Killed with high power shot



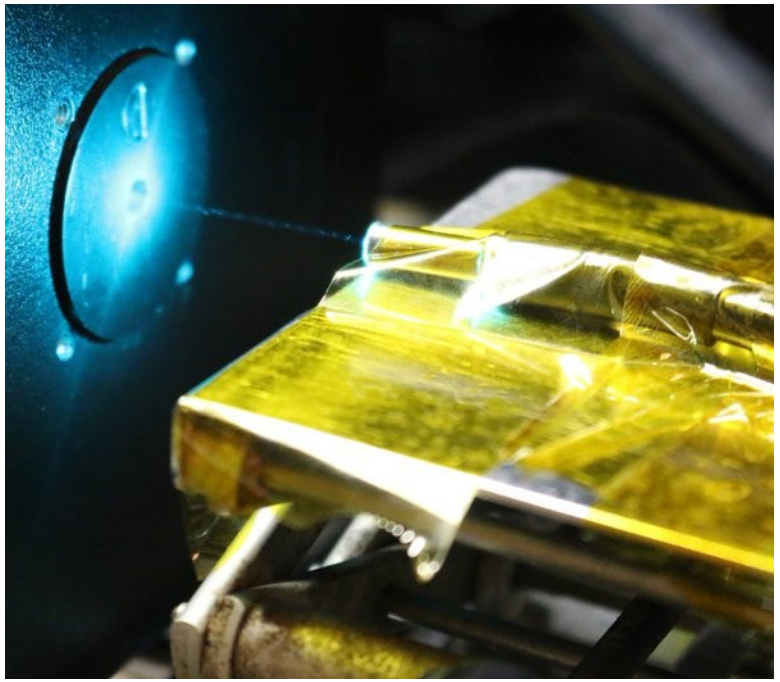


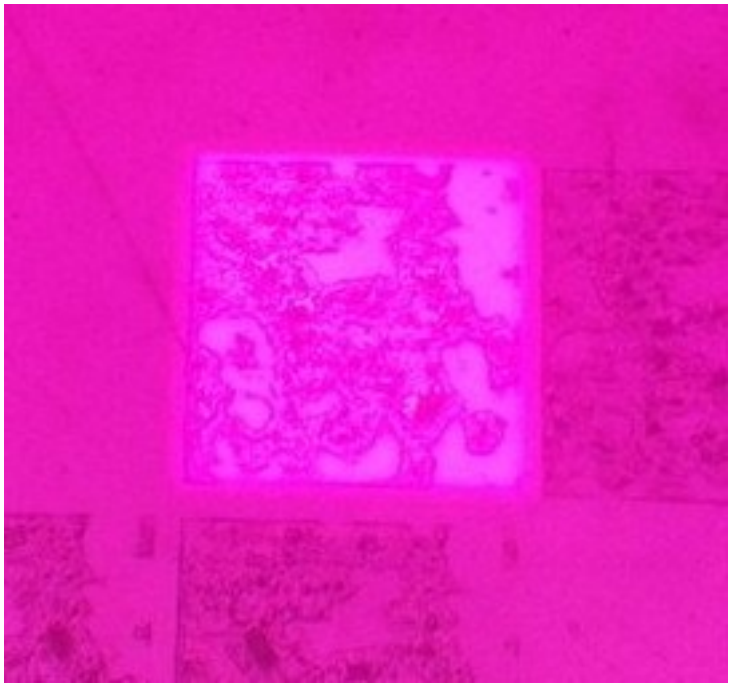


Continuous Wave (CW) lasers

Argon ion

- Injected into ezlaze targeting system
- High losses
- Filters out green => most power => no dice





200 mW 650 nm CW

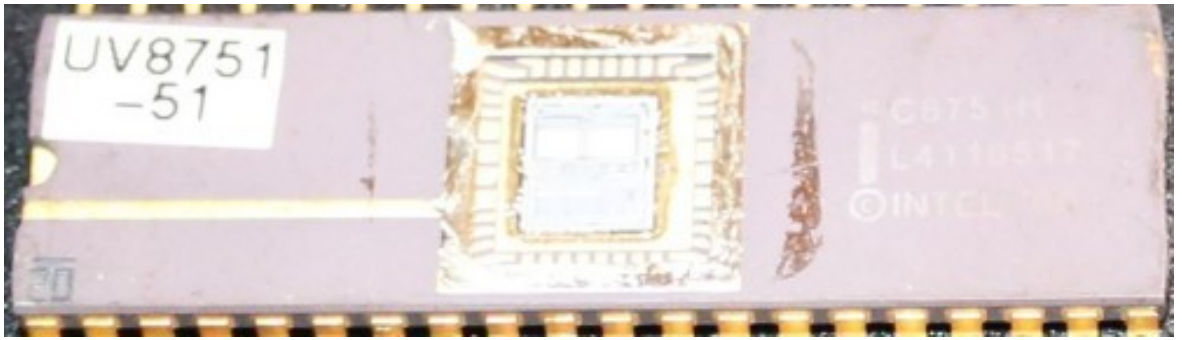
PIC16C57 CW

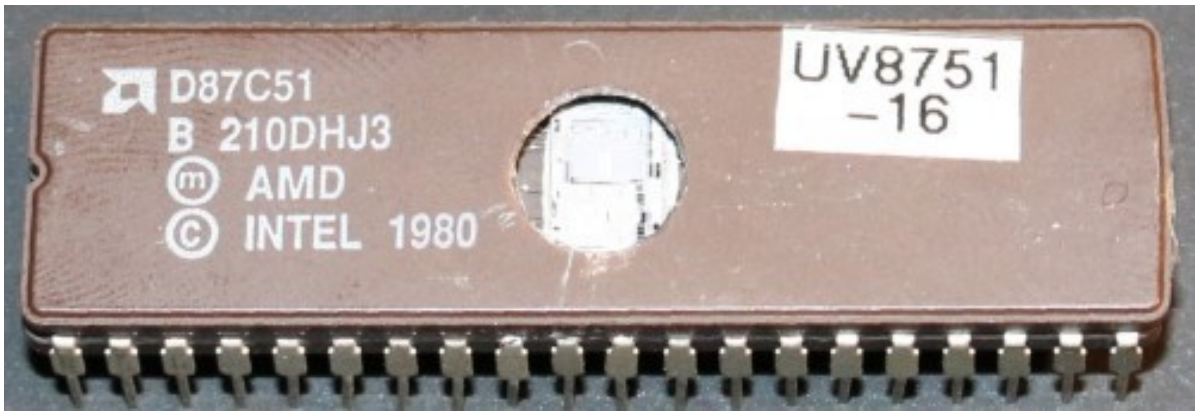
- No code readout but...

```
00000f00  35 32 31 30 39 38 30 38  34 45 45 31 30 43 45 46  |521098084EE10CEF|
00000f10  32 37 41 45 46 46 44 35  32 31 33 45 41 43 38 44  |27AEFFD5213EAC8D|
00000f20  4e 10 ba 01 6b 3e bc ce  11 e2 0b 6e 5d 38 e3 54  |N...k>.....n]8.T|
00000f30  f0 68 d9 69 bc ac c9 80  4d b4 46 73 cf 4a 73 a2  |.h.i....M.Fs.Js.|
00000f40  c6 32 94 f1 00 54 04 5d  7e 1d ee f3 5b 22 a0 7d  |.2...T.]~...[".}|
00000f50  ff 0f ff 0f ff 0f ff 0f  ff 0f ff 0f ff 0f ff 0f  |................|
```

8751 CW

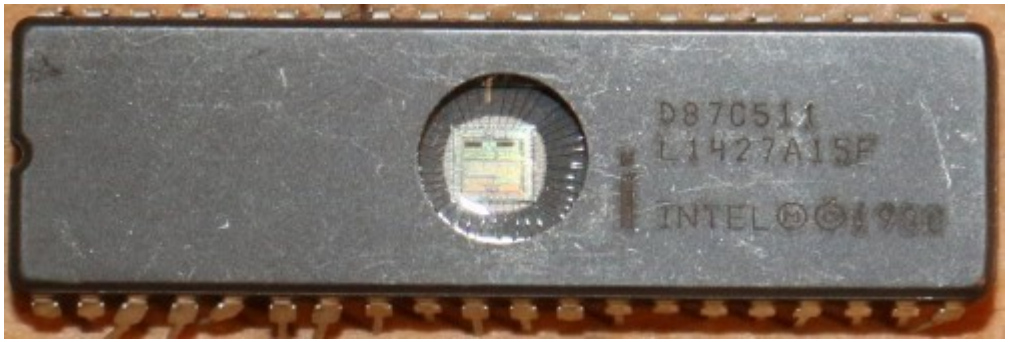
- No dice :(
  - Intel 8751H
  - AMD 87C541B (D87C51)





Intel 87C51 CW

- Works!
  - Intel D87C51I
  - Intel 87C51FA



- Use microscope to find specific location
- Requires laser nearly focused => high power

Intel 87C51 CW demo

CW next steps

- Barely worked: 200 mW => 1000 mW
- CNC scan across die
- Other nm

Summary

- 87C51 break w/ 200 mW red CW laser
- 8751 needs more testing
- PIC16C57 sensitive to Nd:YAG => breakable?
- PIC16C57C in the mail
- I didn't ask you to work for eBay

Thanks for listening!

- Questions? Interested?
  - JohnDMcMaster@gmail.com
- @johndmcmaster