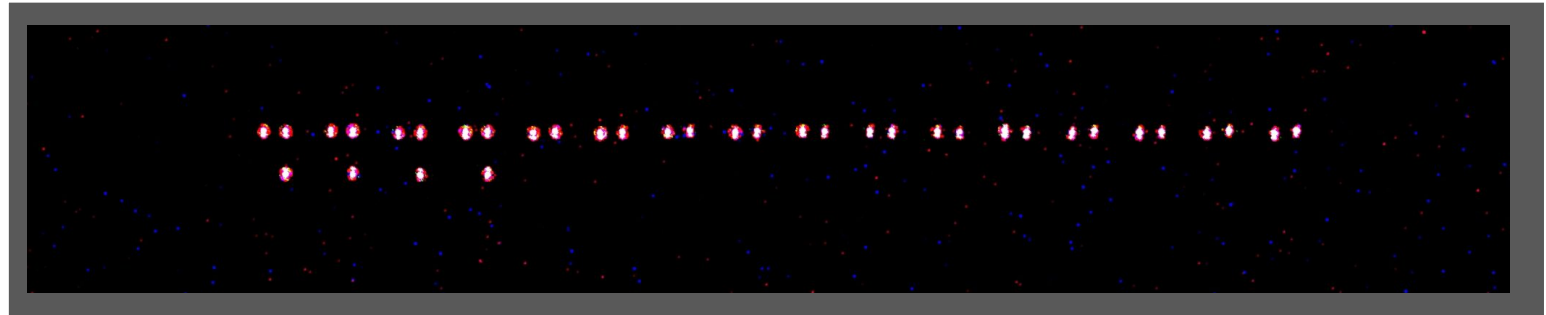


hardwear.io

Extracting programmable logic with photons



John McMaster
McMaster Consulting

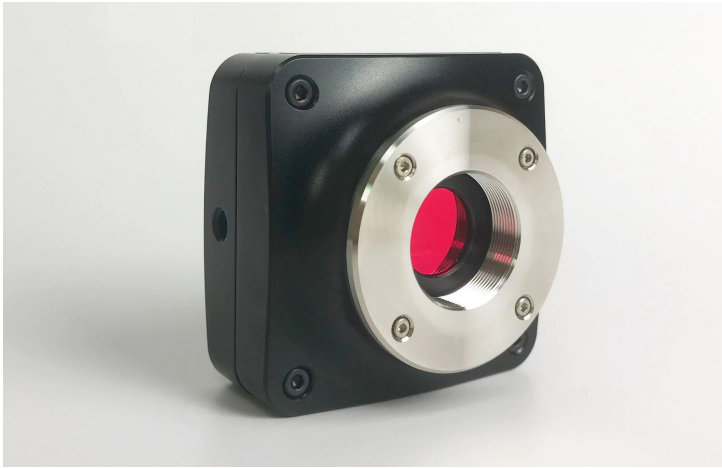
Infrared (IR) emissions

- Emitted during electron recombination
- Emitted at the bandgap of silicon: ~ 1.14 eV \Rightarrow 1088 nm
- Can correlate emissions to circuit activity



Previous talk: use a sensitive \$500 CMOS camera

- Back illuminated CMOS
- Remove IR block filter, install IR pass filter

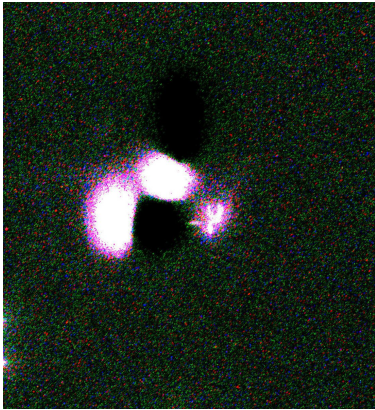


E3ISPM20000KPA

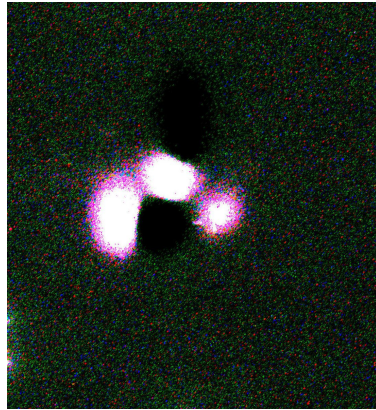


Previous talk: RE bipolar logic based on emissions

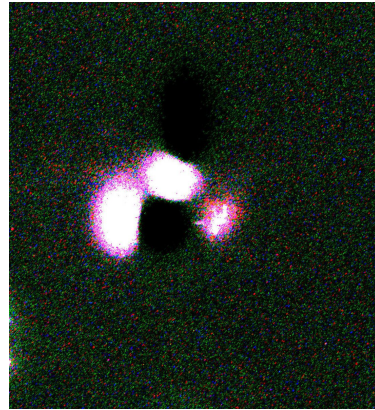
- 2 input NAND gate



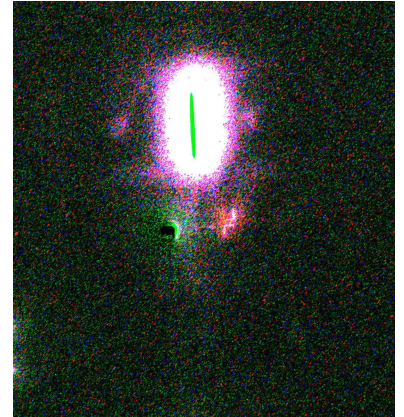
I1: L, I2: L
O: H



I1: H, I2: L
O: H



I1: L, I2: H
O: H



I1: H, I2: H
O: L

This is all good but...

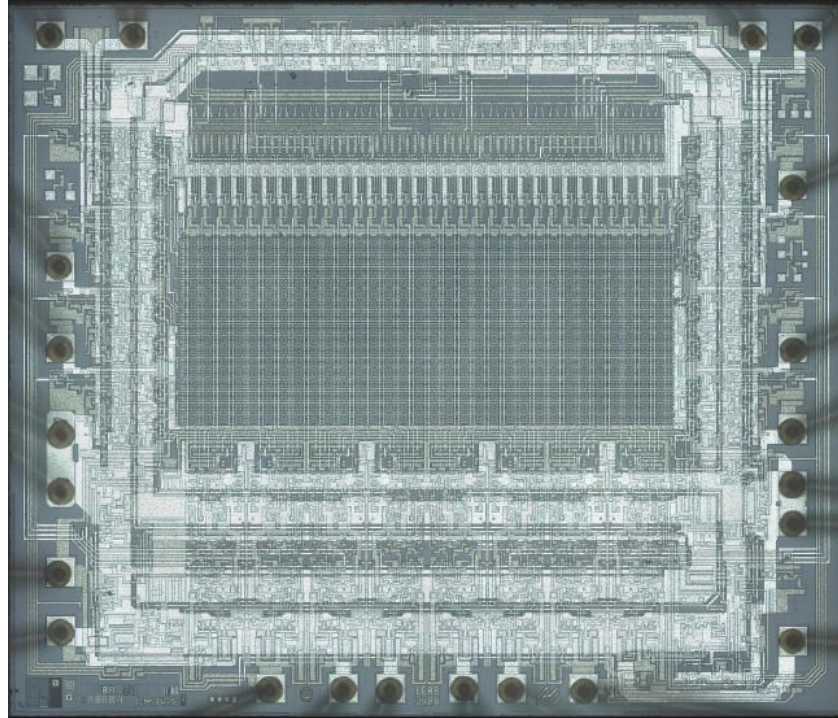
- Research / theoretical on simple devices
- How can we apply this in the real world?
- Get creative: what can we do outside of cryptography?

TrackStar documentation project

- TrackStar 128 allows running Apple][programs on a PC
- Crazy! How does it work?
- Problem: logic devices are protected. What next?

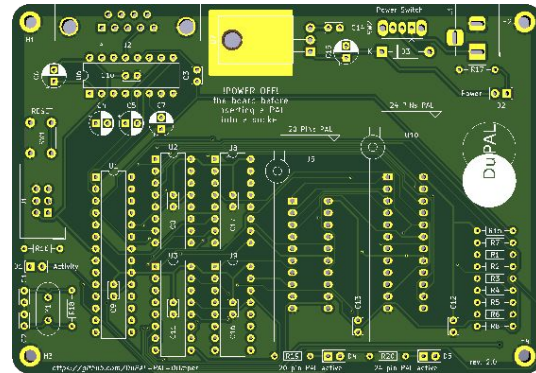
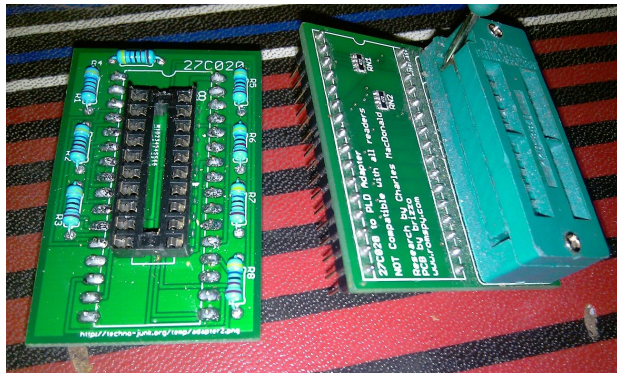


PAL16R8 (DM3428)



Brute forcing PAL devices

- PAL's are relatively simple. Why not just apply all the input permutations?
- Existing projects: readpal, DuPAL, etc
- Played with pal866 (open-tl866) to avoid custom hardware
- May produce equivalent firmware, not the original

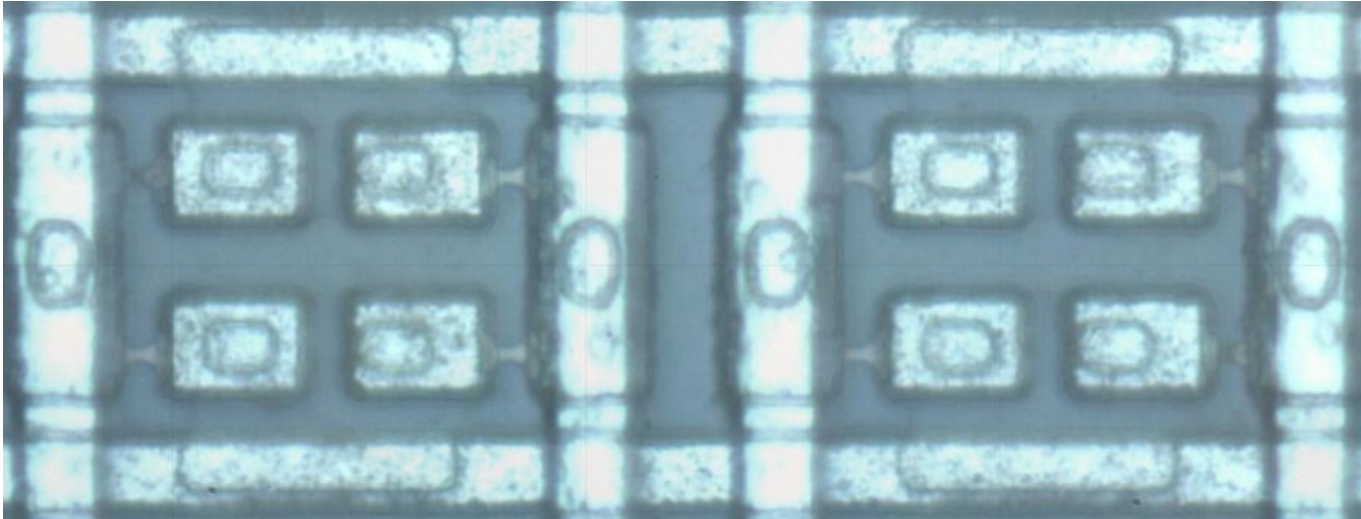


<https://github.com/DuPAL-PAL-Dumper>

<https://www.arcade-projects.com/threads/help-me-solve-an-ssv-mystery.12138/>

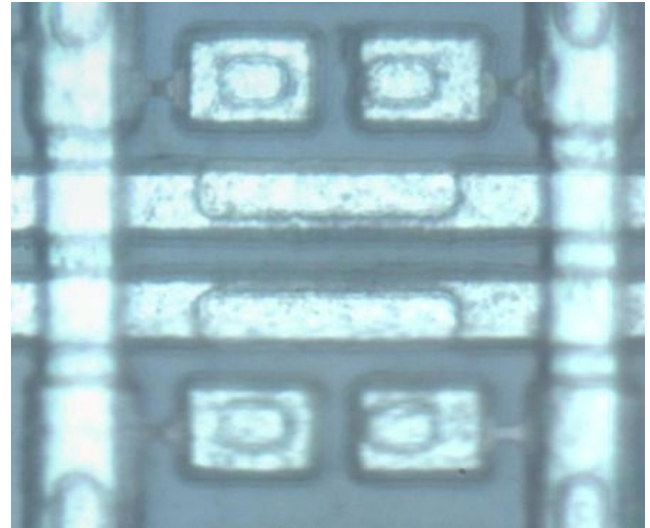
Can it be treated like a mask ROM?

- Yes! Fuses are visible under microscope
- Use existing rompar etc workflow
- But what is the memory layout?



Emissions to the rescue

- Blowing fuse => massive light emission
- Blow one fuse at a time to map memory layout



Automation

- AutoHotkey script drives BP Microsystems GUI
- AutoHotkey TCP server takes JSON from Linux Python program
- Camera in time lapse mode
- Python script synchronized to frame saving



Automation



Abracadabra! inter-word layout

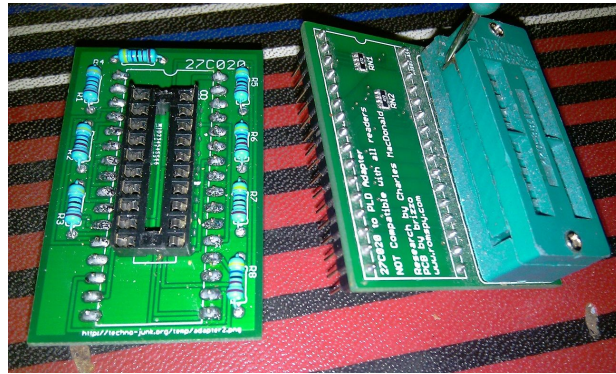


Abracadabra! intra-word layout (word 30)



Verification

- MCU mask ROM => disassemble
- Logic => valid circuits?
- Convert .JED to verilog, compare against test waveforms



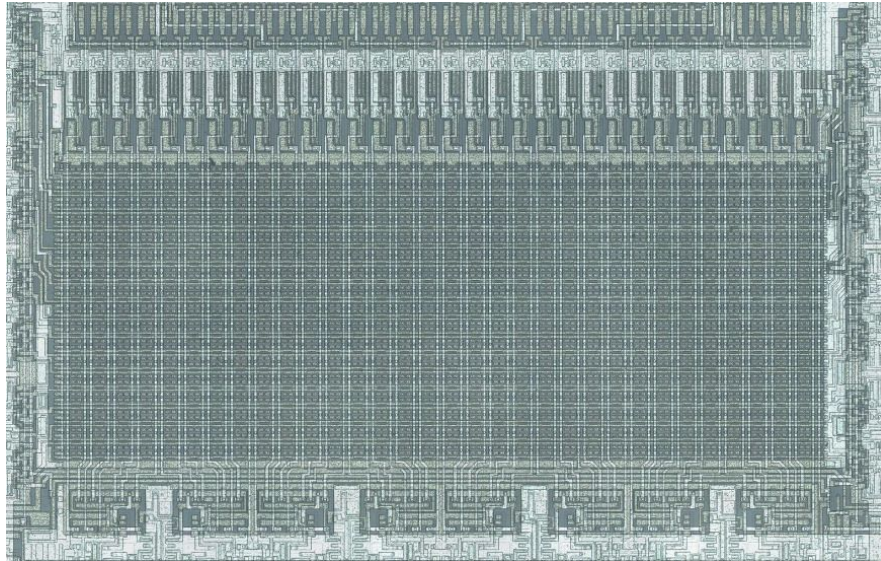
<https://www.arcade-projects.com/threads/help-me-solve-an-ssv-mystery.12138/>

Putting it together

1. Collect test vectors from PAL device
2. Decap PAL device
3. Photograph PAL
4. Convert photographs into bit matrix (manually, rompar, etc)
5. Convert bit matrix to JED using custom Python program
6. Convert JED into Verilog (MAME?)
7. Verify test vectors against Verilog
8. Pretend it worked
9. Do something better

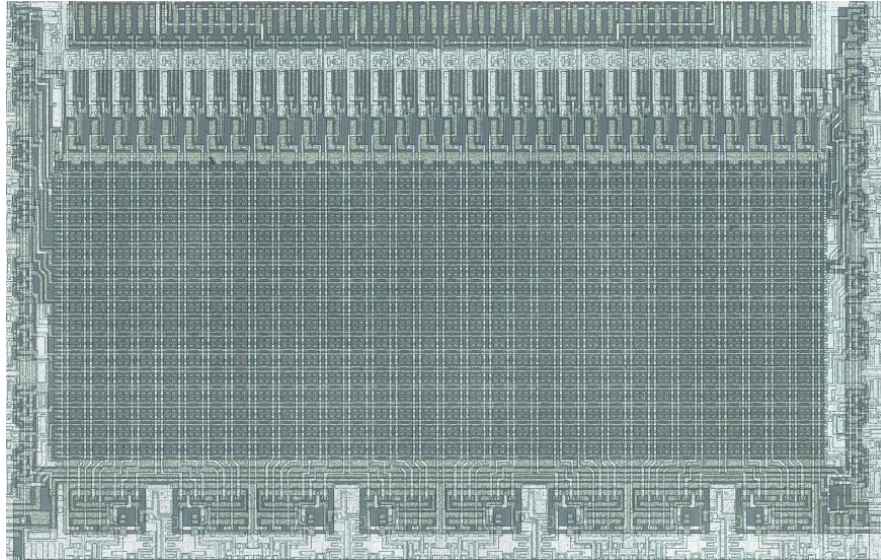
Can we do better?

- If we can instantly locate a fuse, why not just locate the security fuses (2)?
- Theory: they are related to the extra fuses along the edges



Disappointment

- No security fuses visible while burning :(
- Maybe hidden under metal?



Datasheet to the rescue

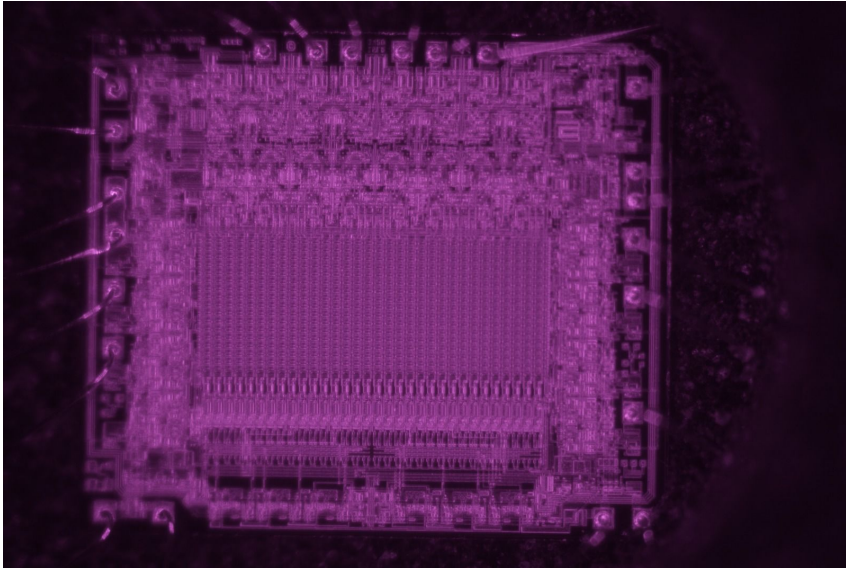
- 1986_National_Programmable_Logic_Design_Guide.pdf

"Note 2: It is recommended that precautions be taken to minimize electrostatic discharge when handling and testing this product. **Pins 1 and 11 are connected directly to the security fuses...**"

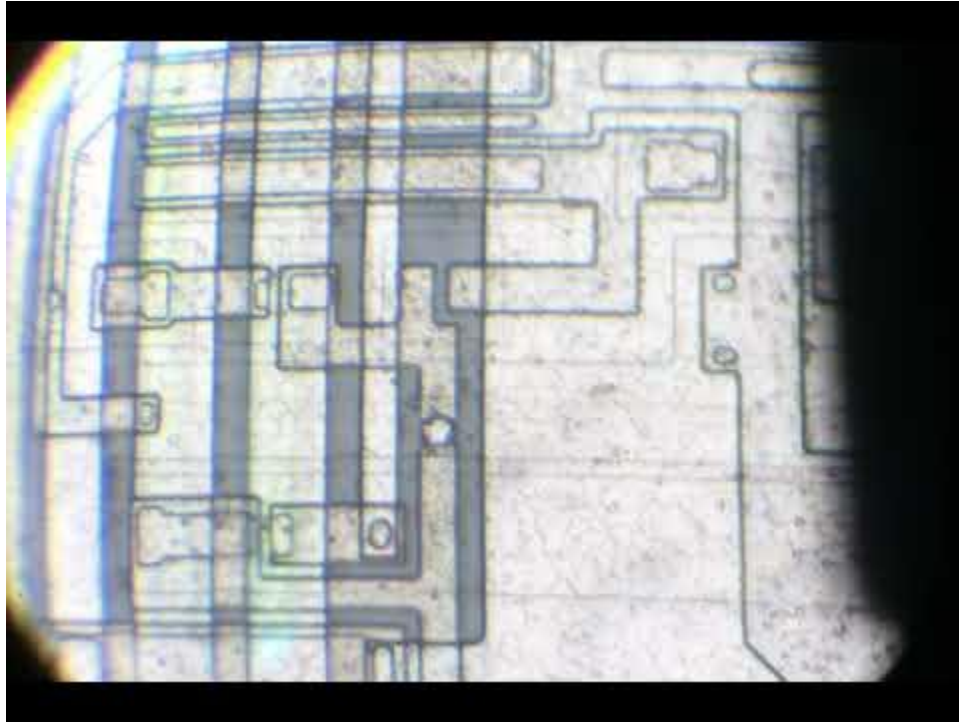
- Let's try again!

Viola!

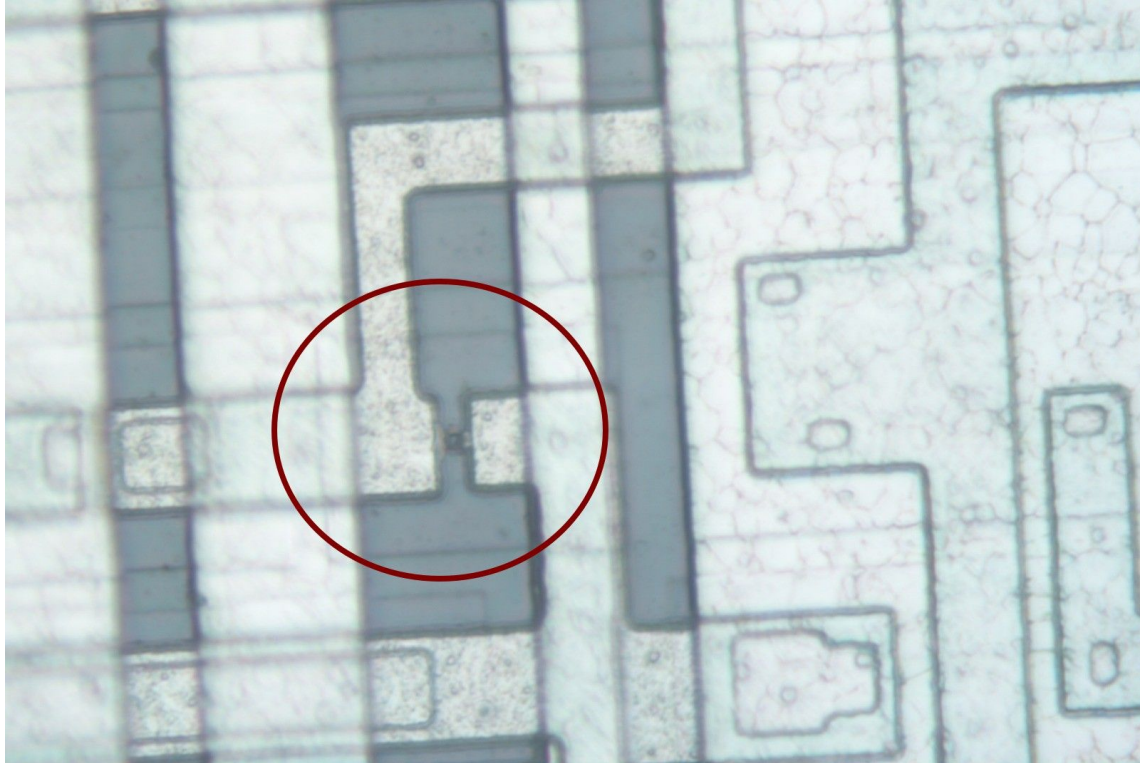
- Two bright spots indicating security fuses



Can we see it burn in real time?



Secured fuse close up



What next?

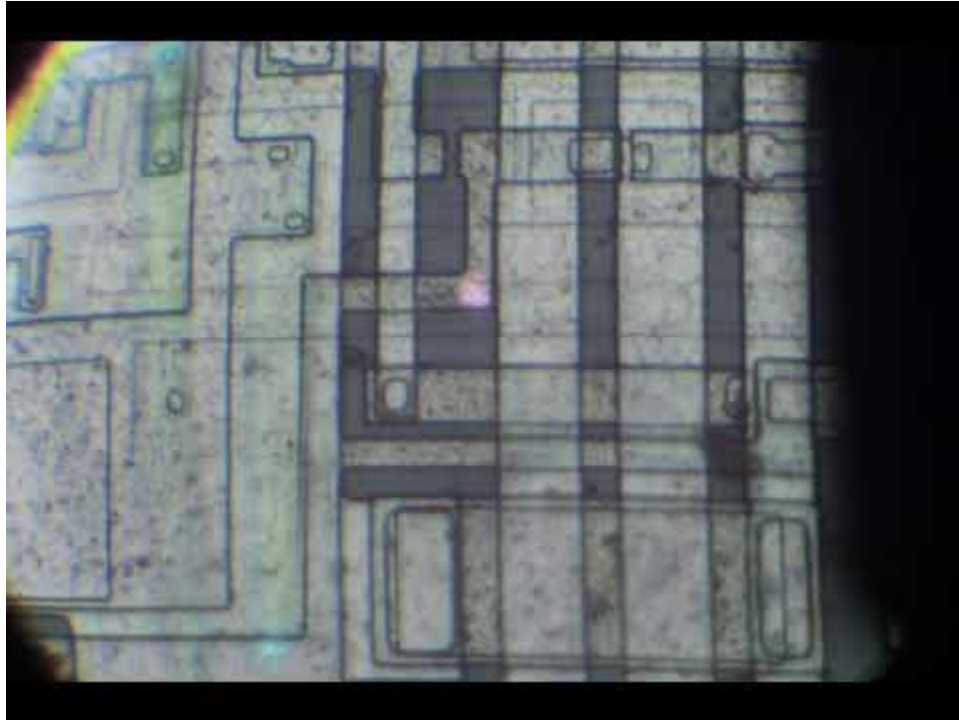
- Microprobe security fuses to remove protection
- How:
 - 1) Use laser probe station to cut holes in overglass to expose metal
 - 2) Microprobe exposed circuit traces to force logic value

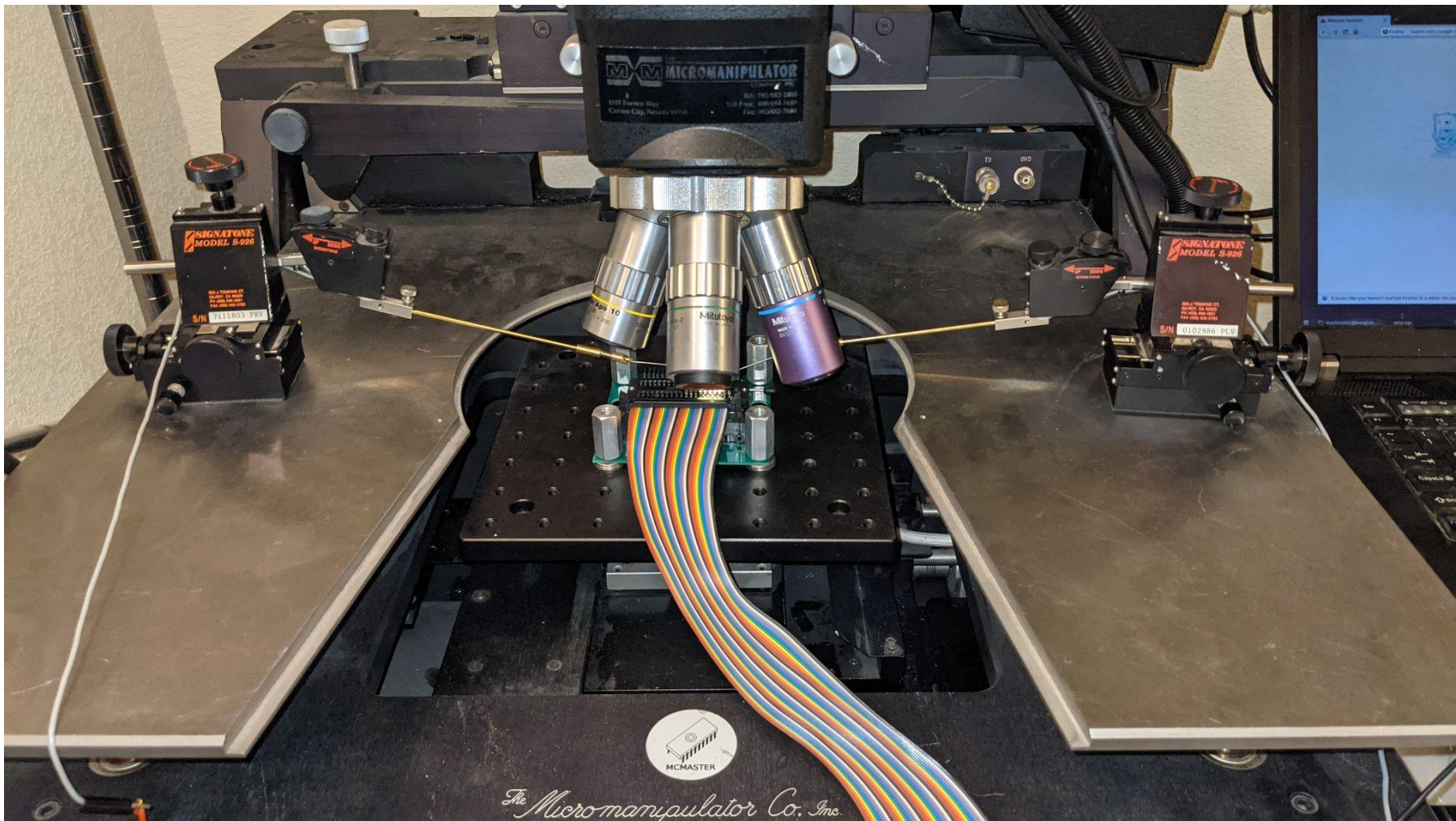
How to probe?

- Take scope traces before / after security to understand logic states
- Ideally constant value (VCC/GND) => don't need to actually bridge fuse
- Old/big logic => not using active probes



Time to put some photons in





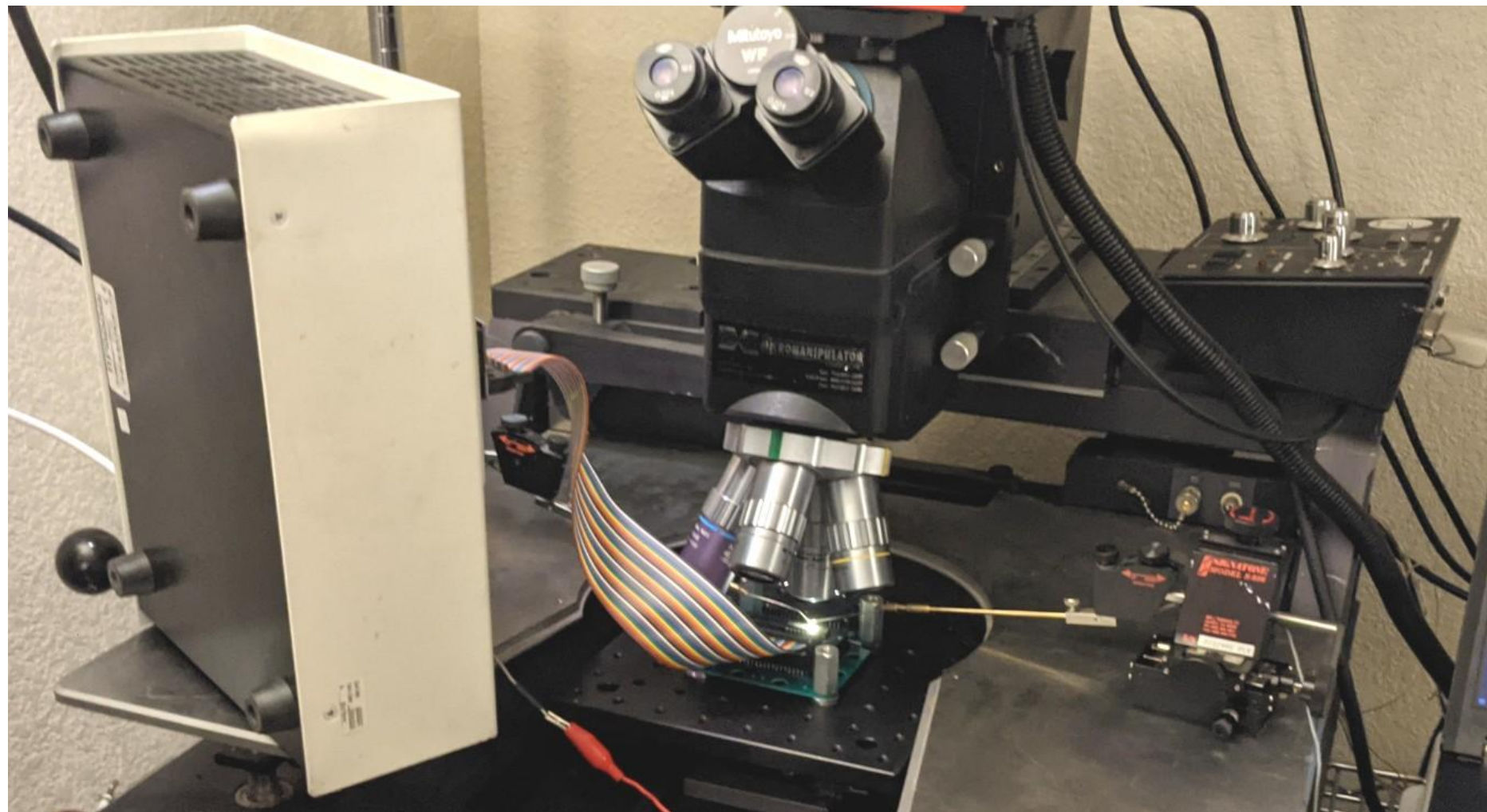
MM MICROMANIPULATOR
CORPORATION
8000 Paradise Way
Carson City, Nevada 89704
Tel: 702/733-2800
Toll Free: 800/543-5497
Fax: 702/482-7688

SIGNATURE MODEL S-926
Piezo Transducer
S/N 7111803-PRV

SIGNATURE MODEL S-926
Piezo Transducer
S/N 0102966-PLV

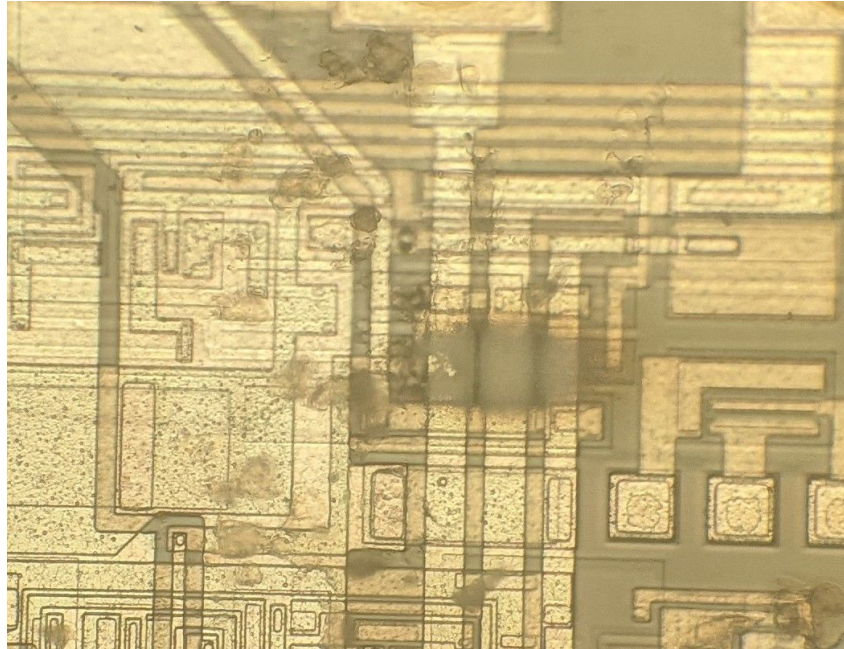


The Micromanipulator Co., Inc.

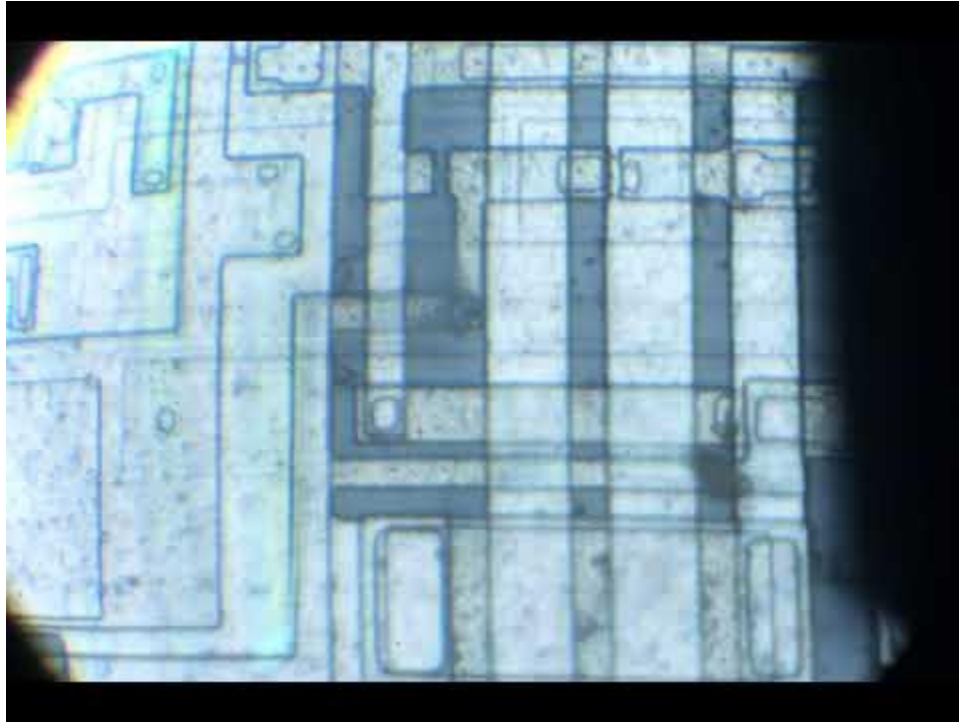


Oopsie daisy...short circuit

- Tungsten probe somehow melted before the IC trace!

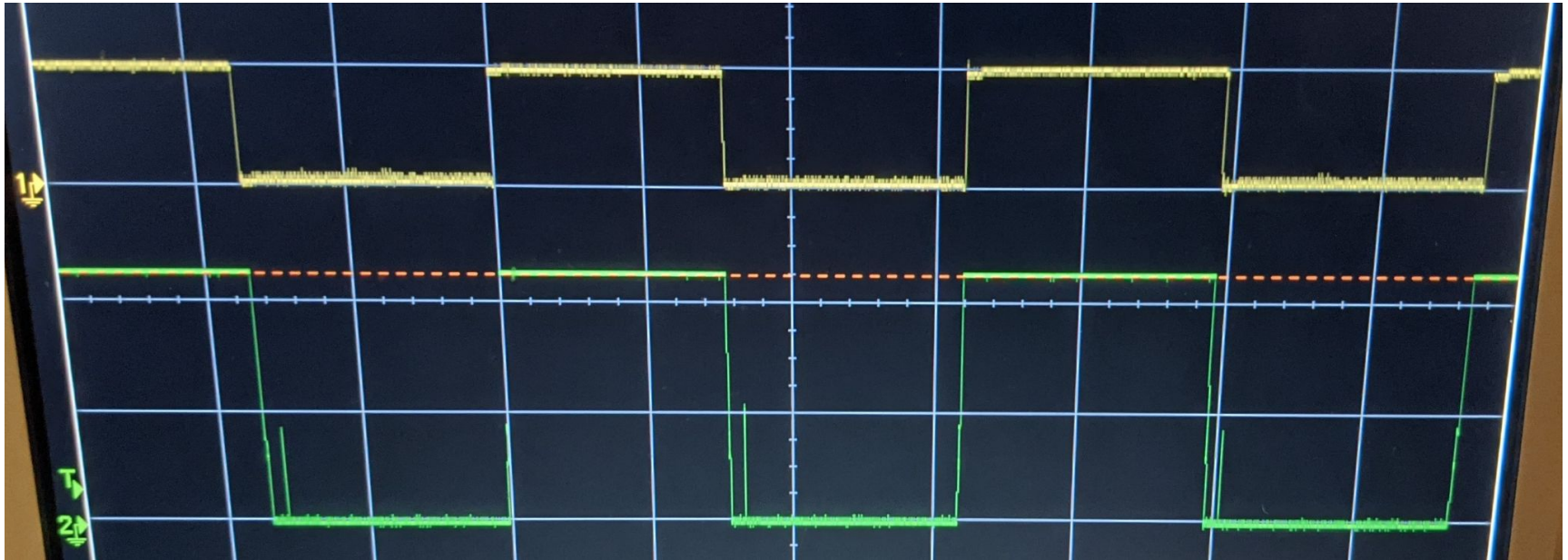


Try probing again...



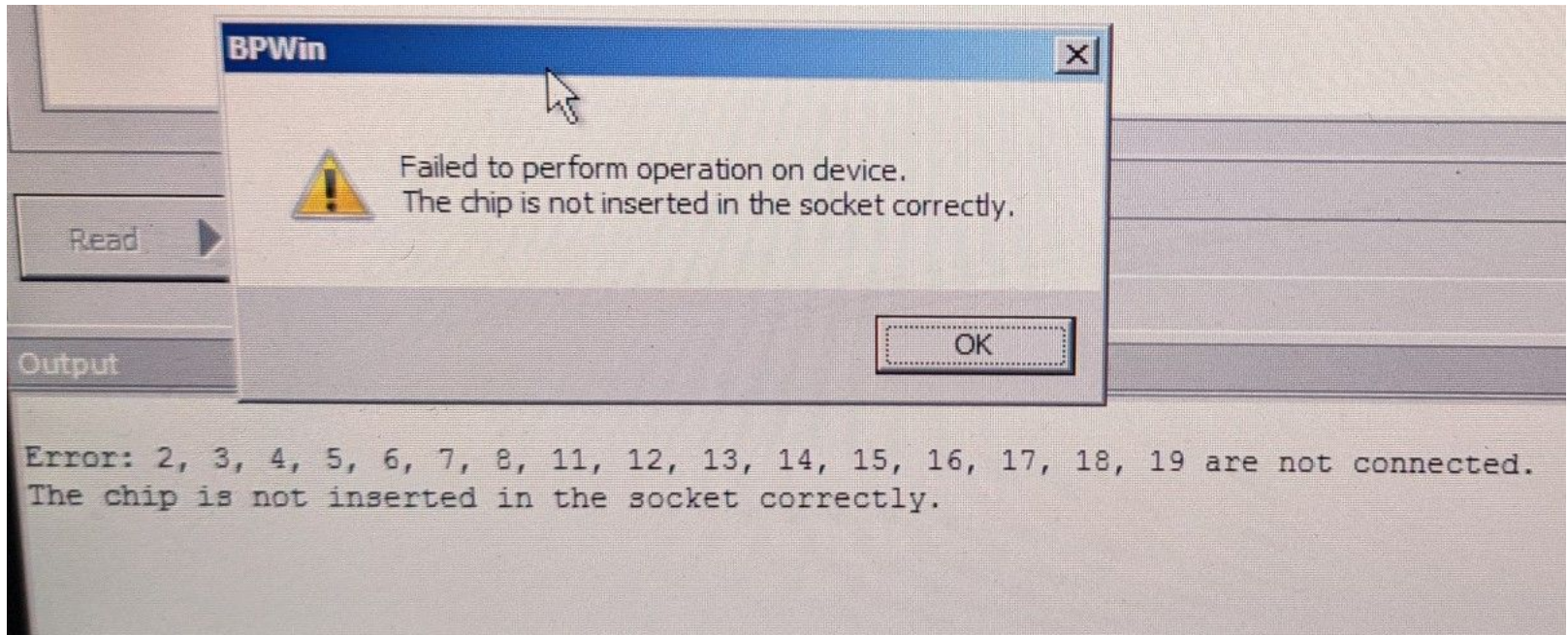
An unexpected result

- Not constant VL or VH => analog / specialized circuit?
- 5V (inner die) and ~12V (outer die) observed



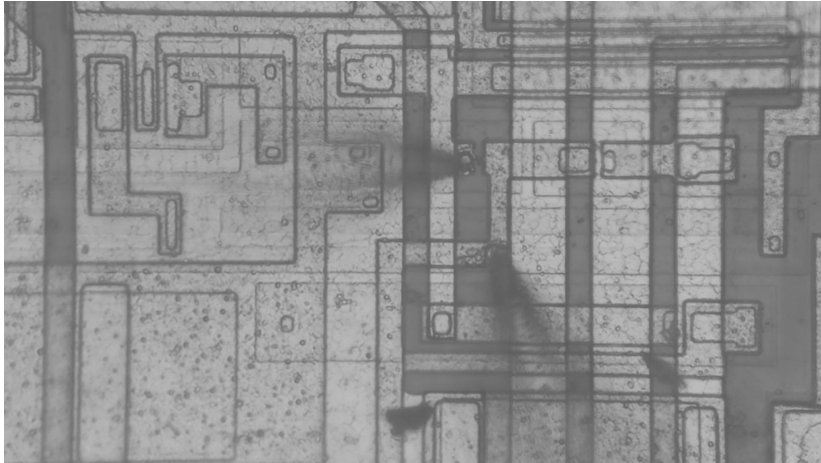
External power made it sad

- Tried both sides



...so just bridge the contacts w/ two microprobes

- Success! But half of the data => do twice
- PoC here but also worked on Trackstar PAL16R8

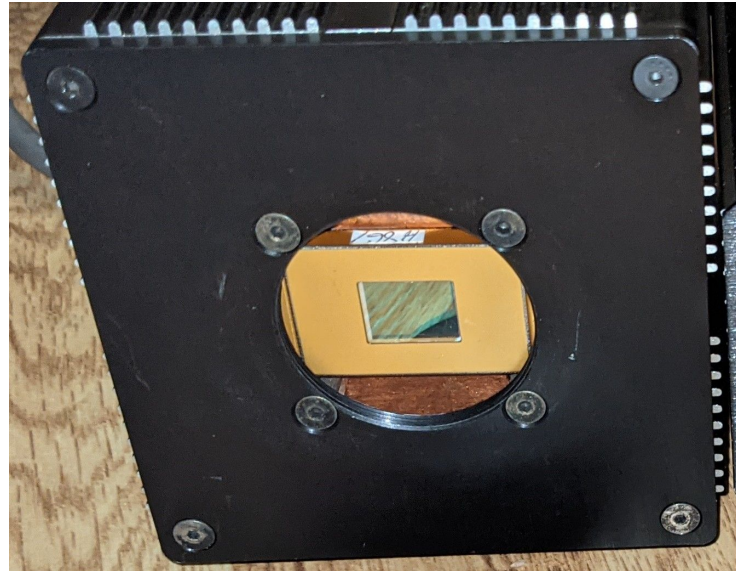


```
000h: 0000000 1000000 0100000 1100000 0010000 1010000 0110000 1110000
040h: 0001000 1001000 0101000 1101000 0011000 1011000 0111000 1111000
080h: 00001000 10001000 01001000 11001000 00101000 10101000 01101000 11101000
0C0h: 00011000 10011000 01011000 11011000 00111000 10111000 01111000 11111000
100h: 00000100 10000100 01000100 10000100 00100100 10100100 01100100 11100100
140h: 00010100 10010100 01010100 11010100 00110100 10110100 01110100 11110100
180h: 00001100 10001100 01001100 11001100 00101100 10101100 01101100 11101100
1C0h: 00011100 10011100 01011100 11011100 00111100 10111100 01111100 11111100
200h: 00000010 10000010 01000010 10000010 00100010 10100010 01100010 11100010
240h: 00010010 10010010 01010010 11010010 00110010 10110010 01110010 11110010
280h: 00001010 10001010 01001010 11001010 00101010 10101010 01101010 11101010
2C0h: 00011010 10011010 01011010 11011010 00111010 10111010 01111010 11111010
300h: 00000110 10000110 01000110 11000110 00100110 10100110 01100110 11100110
340h: 00010110 10010110 01010110 11010110 00110110 10110110 01110110 11110110
380h: 00001110 10001110 01001110 11001110 00101110 10101110 01101110 11101110
3C0h: 00011110 10011110 01011110 11011110 00111110 10111110 01111110 11111110
400h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
440h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
480h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
4C0h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
500h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
540h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
580h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
5C0h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
60h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
640h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
680h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
6C0h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
700h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
740h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
780h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
7C0h: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```


Epilogue (if time)

Need better camera for more modern applications?

- InGaAs cameras! Non-silicon IC
- More sensitive but short exposure time :(
- Neither useful in practice



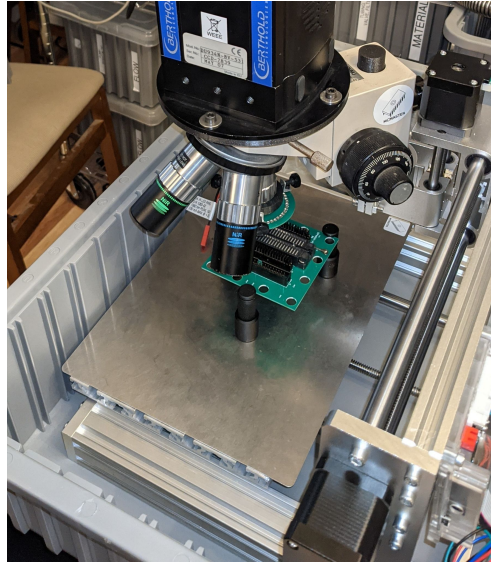
What else is out there?

- Last time: cooled camera had low noise, but CMOS had best sensitivity
- Could we get a cooled CMOS detector? Yes!
- \$\$\$ but scrapped out of surplus medical device
- Special thanks to Bayley of [oneTesla](#) for loaning me this camera!



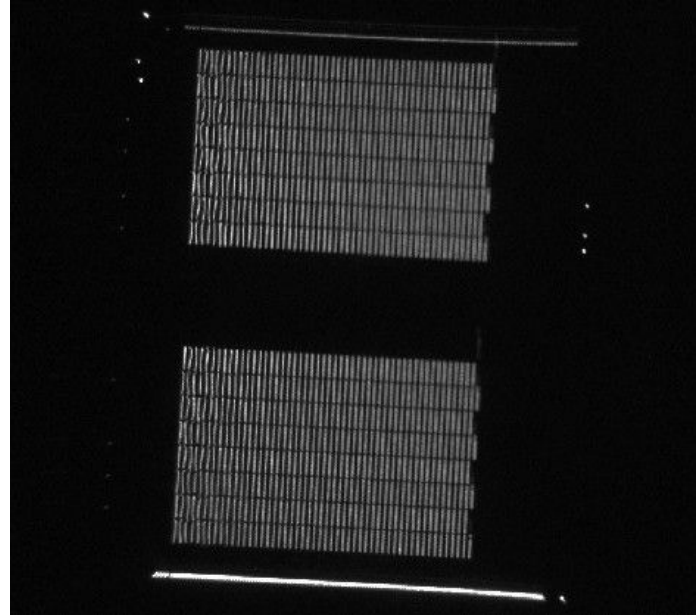
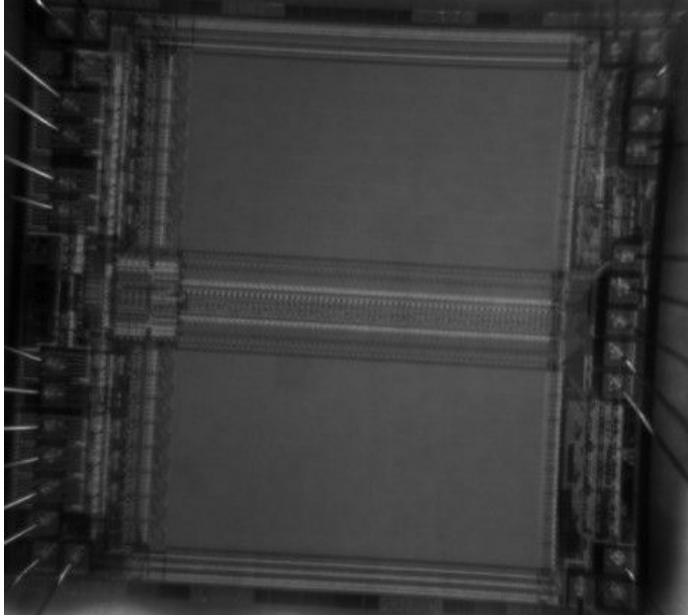
Improved enclosure

- Mount camera on low cost CNC to manipulate in the dark
- More properly sealed enclosure



EPROM / flash?

- EPROM plausible, flash no
- TODO: EPROM security fuse (ex: 8751, PIC)



Future work

- Antifuse
- EPROM security fuses
- Bridge w/ silver epoxy?



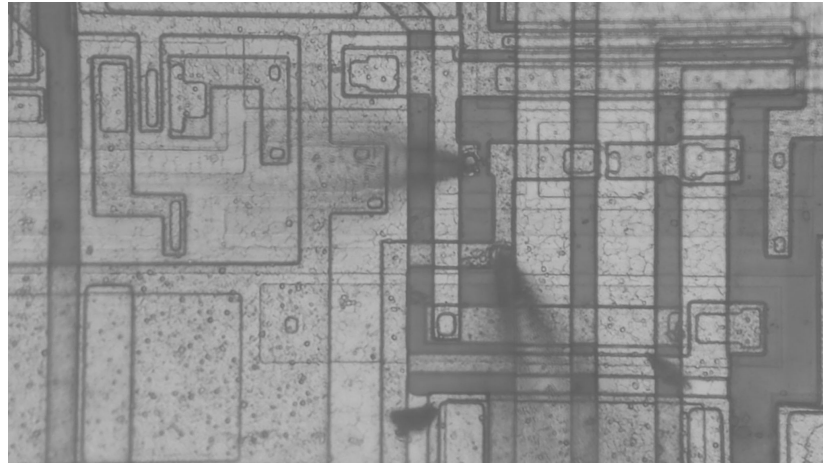
Special thanks

- Ethan Wright: helping with lab work
- Bayley Wang: cooled Apogee camera
 - <https://onetesla.com/>
- Brandon Cobb: Trackstar support, partial funding
 - <http://www.diskman.com/>



Thanks for listening!

- @johndmcmaster
- BP Microsystems AHK: <https://github.com/JohnDMcMaster/bpmicro>
- pal16 scripts: <https://github.com/JohnDMcMaster/icfuzz>
- pal866: <https://github.com/JohnDMcMaster/pal866>



Backup

Summary

- Fuse burning readily visible under microscope
- EPROM was visible in some of my tests
- Flash was not visible in my tests

Demo?

- Questions first?
- Step 1: find fuses
- Step 2: microprobe security

Bit matrix to Verilog workflow

- `python3 txt2jed.py capture.txt capture.jed`
- `jedutil -convert capture.jed capture_mame.bin`
- `python3 pal16r8_to_verilog.py capture_mame.bin >capture.v`

Laser settings

- Green, High-650
- Marker around 2.25 / 2.25

An unexpected result

- Not VL or VH => analog / specialized circuit
- Options:

1) Emulate voltage externally

2) Bridge fuse(s)

	Blank	Secure (outer)	Secure (inner)
Left	1.62V	1.70V	Oops
Right	1.55V	1.47V	0.01V