Integrated-Circuit Surgery:
getting to the heart of the problem with the smallest scalpel

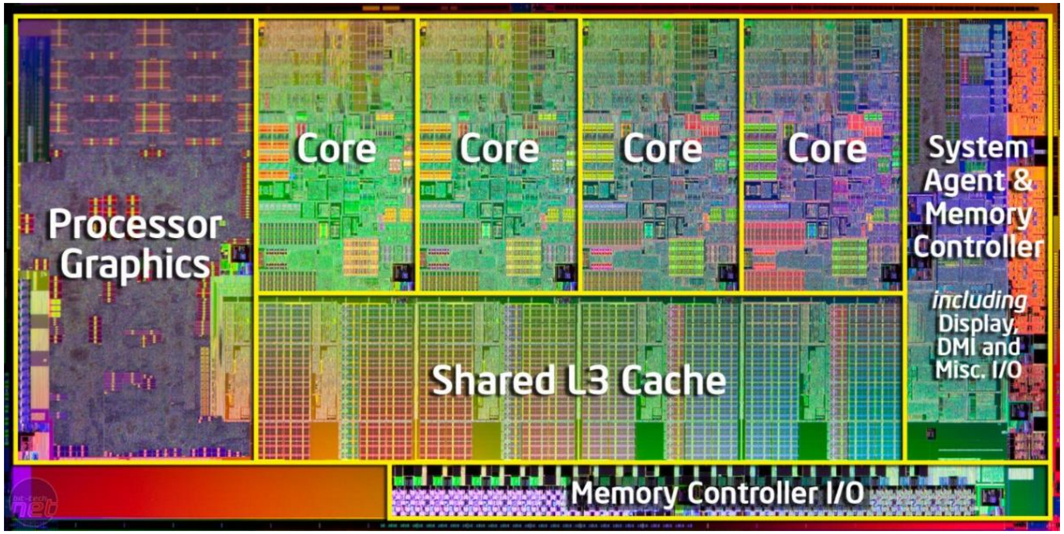
John Walker

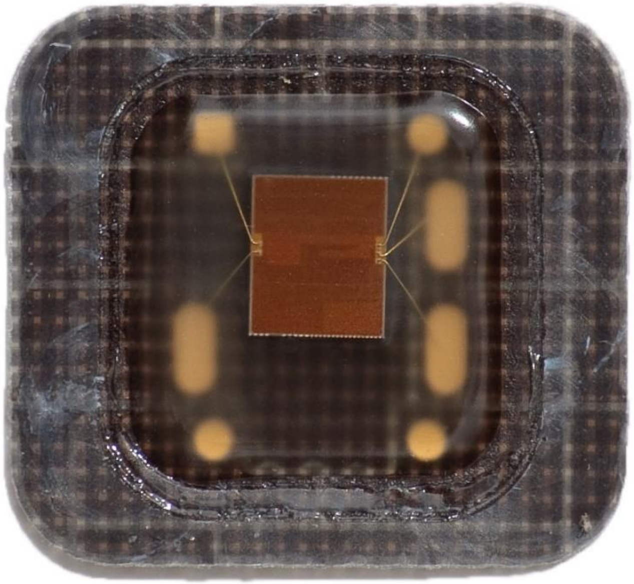
Hardware.io
The Hague, Netherlands
September 2019

The need for secure hardware

- Software, Firmware and Hardware. All can contribute to making a microchip secure
- Software, Firmware and Hardware. They can all equally contribute to making a secure microchip insecure
- This talk concentrates on hardware security and on the physical aspects of that security
- A chip can be hacked given enough time, effort and resources. The defender is tasked with ensuring that the expenditure of time, effort and resources is greater than any gain from a successful attack

Different forms of secure hardware: Hard versus hardened





- The typical microprocessor is hard because it is complex
- Small geometry down to 7nm
- Billions of elements
- Complex data flow, but designed for speed and efficiency with security down the list

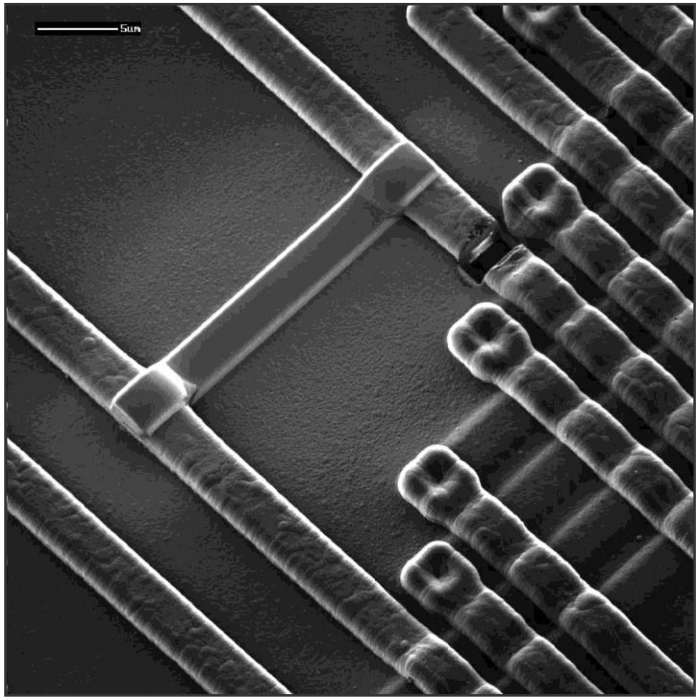
- A secure chip is hardened but might not be complex
- Limited number of features
- Secure shields
- Security is the first priority

What does hardened mean?

- Software and Firmware are designed to prevent known attack paths. Internal firewalling, error checking and obfuscation are used to stop attacks
- Features such as true random number generators are used
- Test and analysis functions such as JTAG are either not present, disabled or cryptographically secured
- A secure chip is normally protected against probing attacks using a shield or system of shield.

Physical attacks

- Probing
- Rewiring
- Focused ion beam
- Changing the chip behaviour to do what you want



Focused Ion Beam Workstation

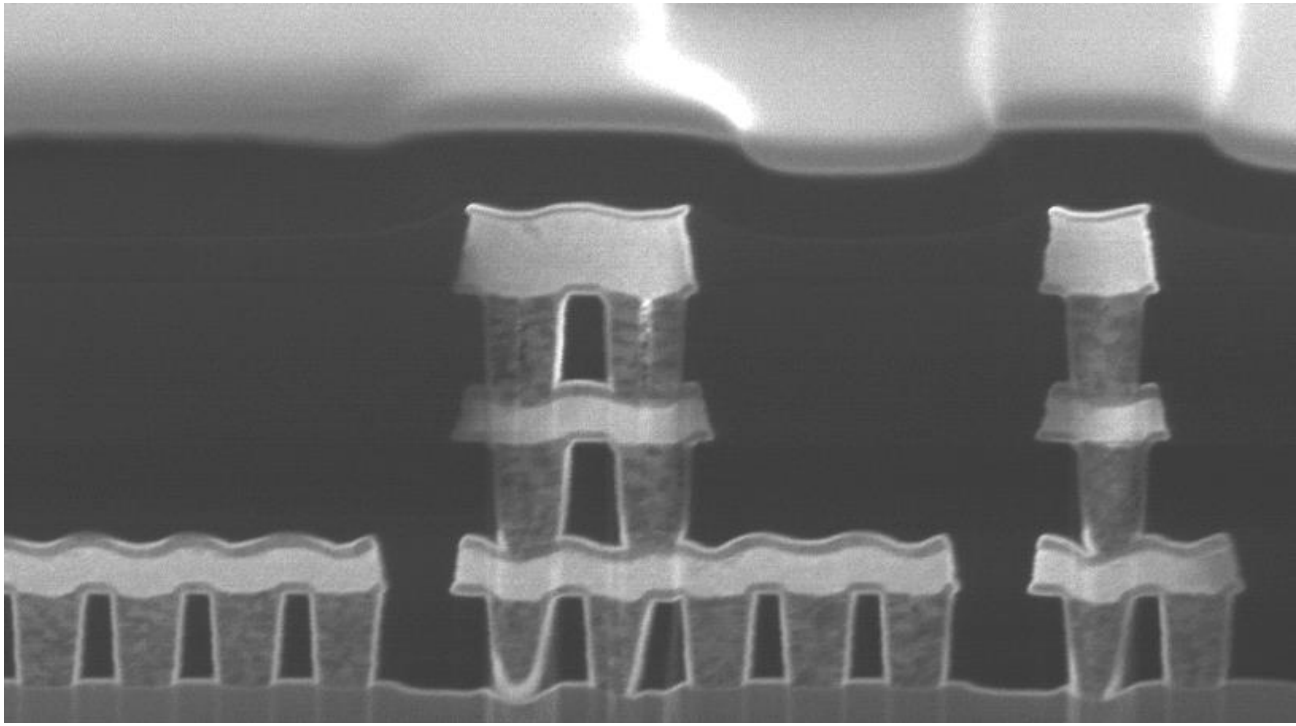
- First it is a microscope
  - An ion microscope with 5nm resolution
  - An electron microscope with sub-nanometer resolution
  - An infra-red microscope to look through silicon
- Second it is a digging tool
  - The Ga ion beam can sputter away material with significantly sub-micron resolution
  - It can selectively remove different materials (aluminium, copper, dielectric)
- Third it can add new circuit to your chip
  - Deposit new conductive tracks and probe points using metal deposition
- Changing the chip behaviour to do what you want

Stages in an attack

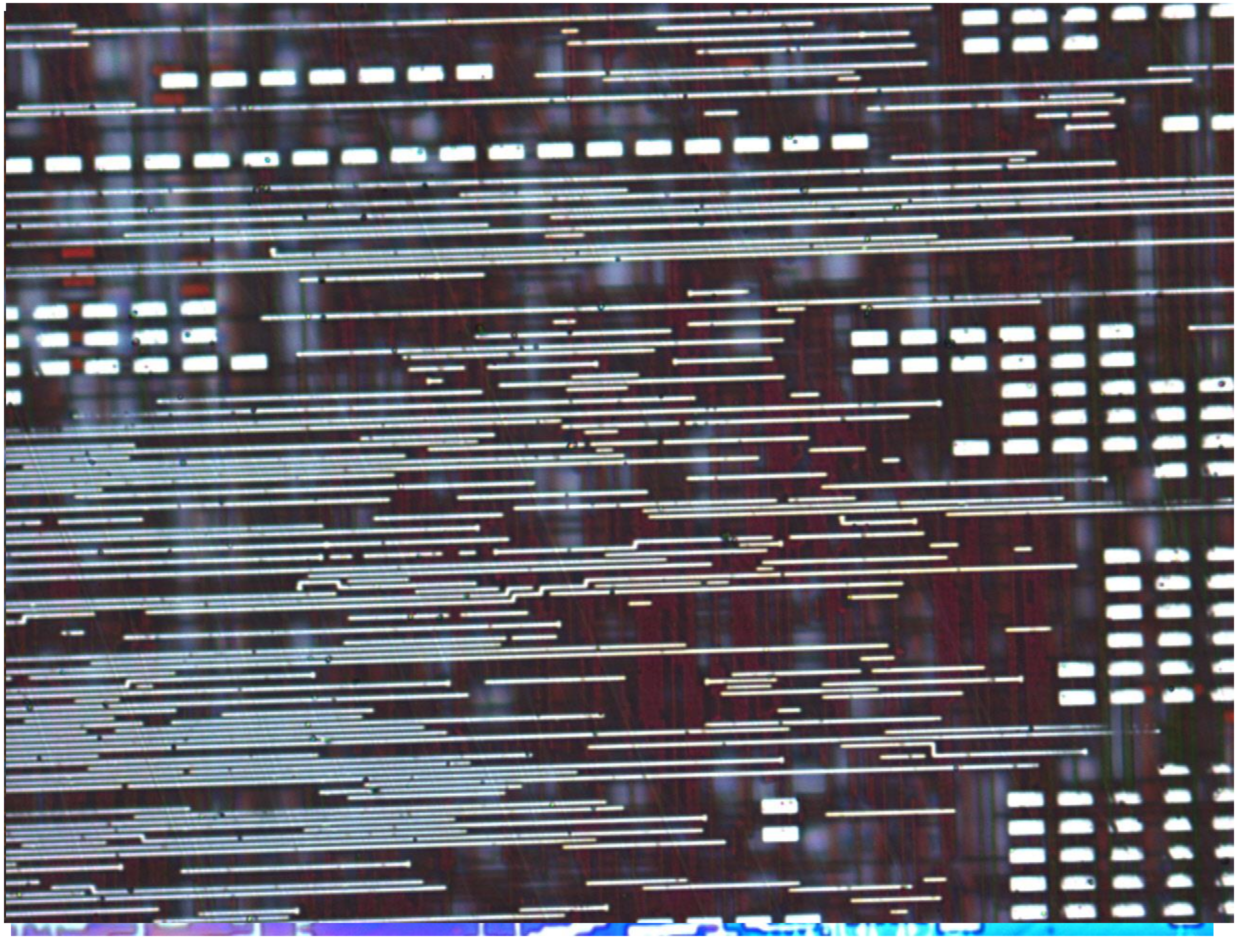
1. Are you testing security, breaching security or researching security?
2. Find out what is there first
   - Read available documentation (maybe not much)
   - Reverse engineer the chip
3. Identify the potential weaknesses and try to exploit them
4. Change the chip behaviour to do what you want

Reverse Engineering

- Reverse engineer to make a 3 dimensional map of a chip
  – Many chips die, but their sacrifice guarantees them a place in heaven
- Strip back layer-by-layer
  – Wet chemical etching
  – Mechanical grinding and lapping
  – Reactive ion etching
- Capture an image of each layer, including all gates, interconnects and vias
- Identify the functions of blocks, cells/gates and structures
  – Identify how the above are interconnected
  – Identify weak points

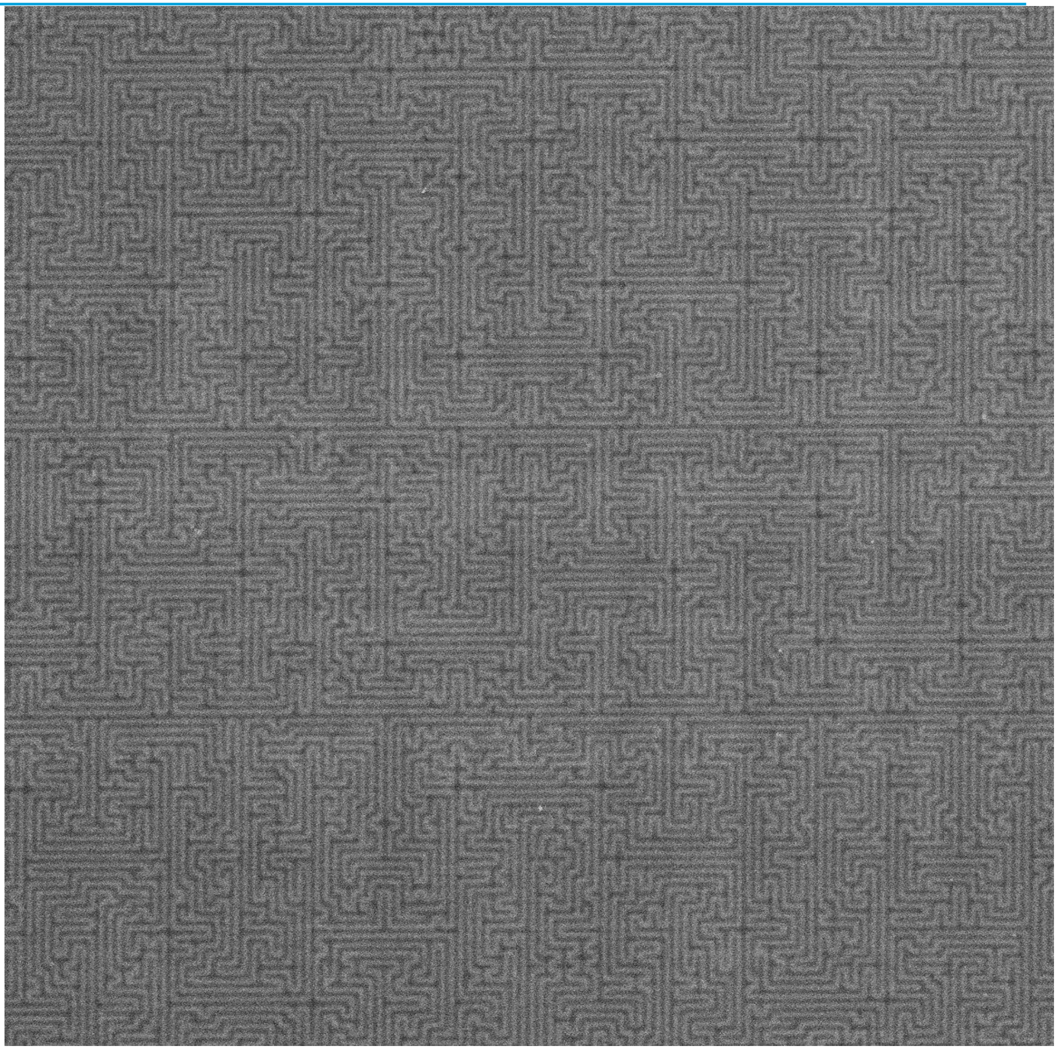


Strip back layers



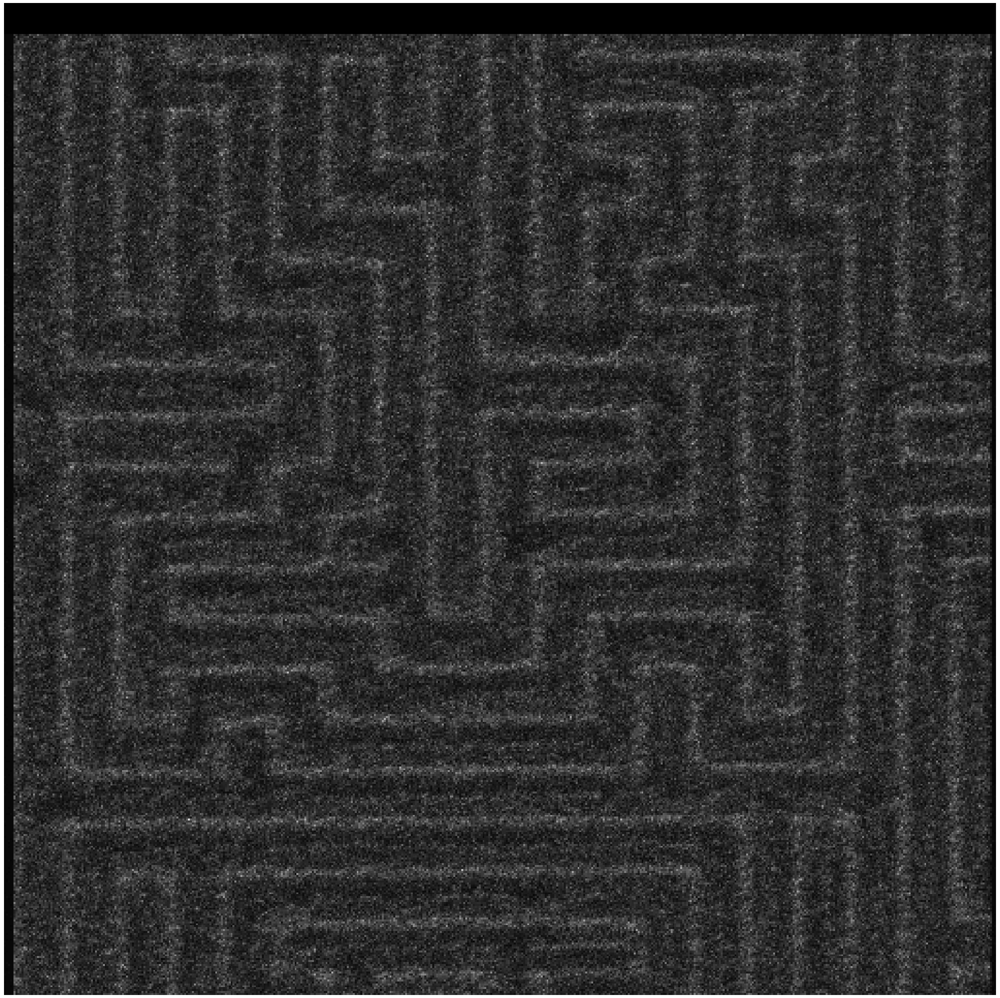
Active security shields

- Prevention of probing attacks
- Top one or two layers are shield
- Multiple active circuits
  - If any circuit is cut (open-circuit) then the chip is disabled
  - If any two adjacent circuits touch (short-circuit) then the chip is disabled
- The chip only recognises fault when it is powered up



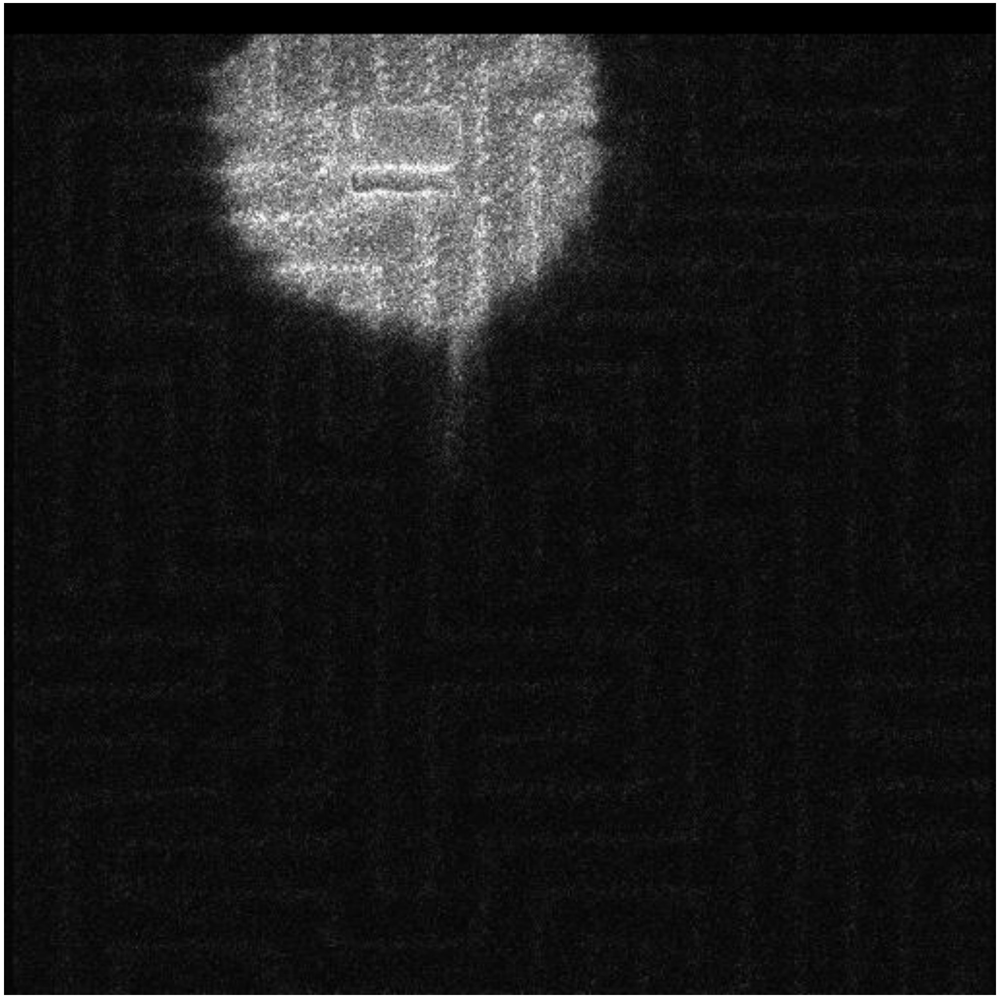
Limited area attacks

Used to remove the active shield from above a single point for probing.



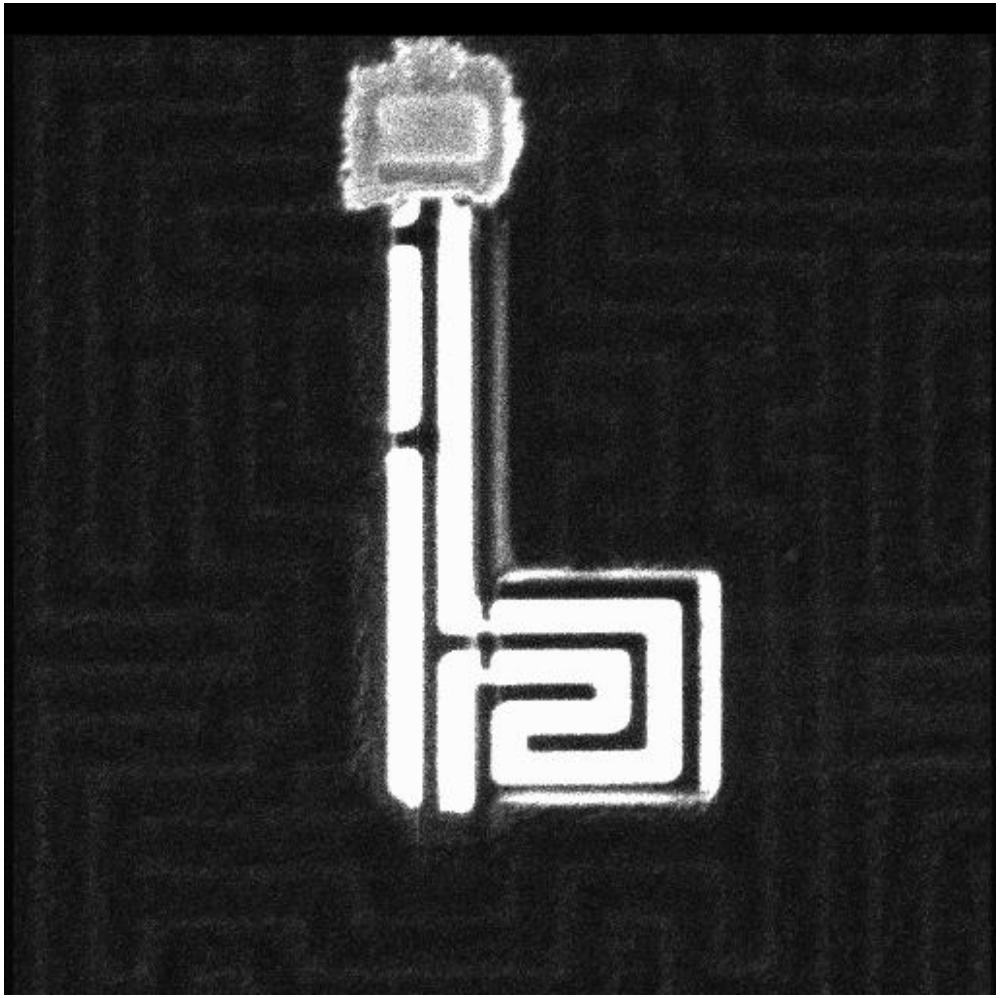
Bridge shield lines

A loop in the active circuit can be short-circuited without affecting the circuit.



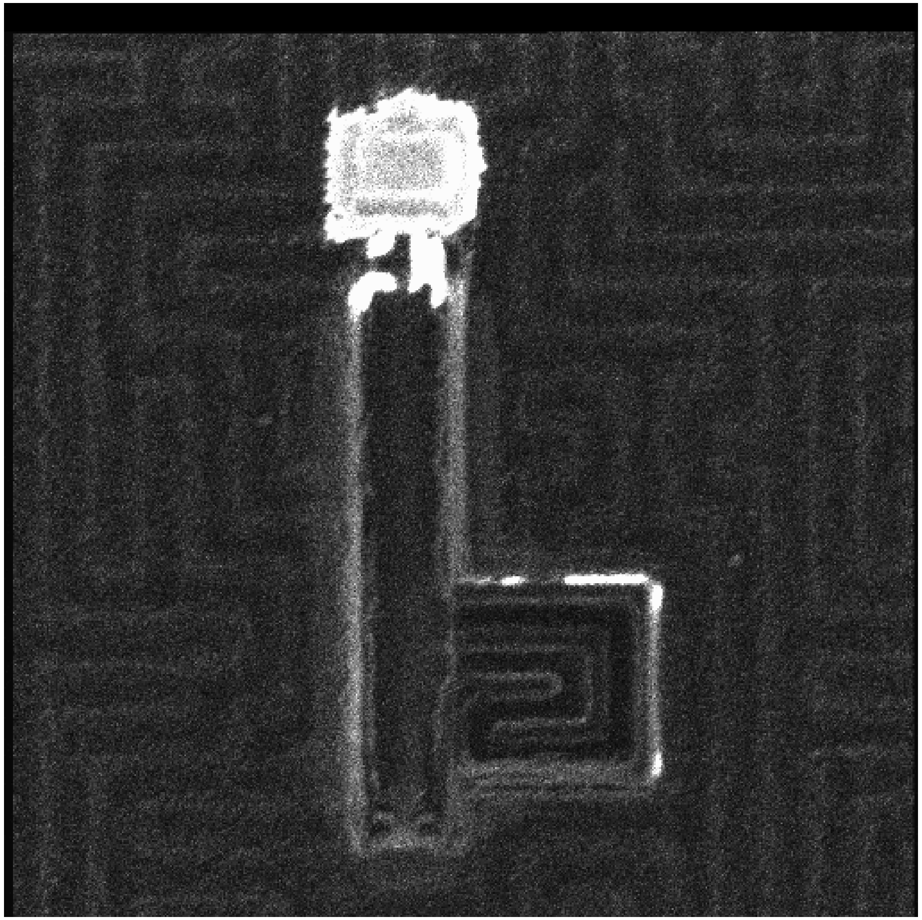
Expose shield area to be removed

The loop can be exposed. It is then possible to remove the loop material without a breach being detected.



Remove shield

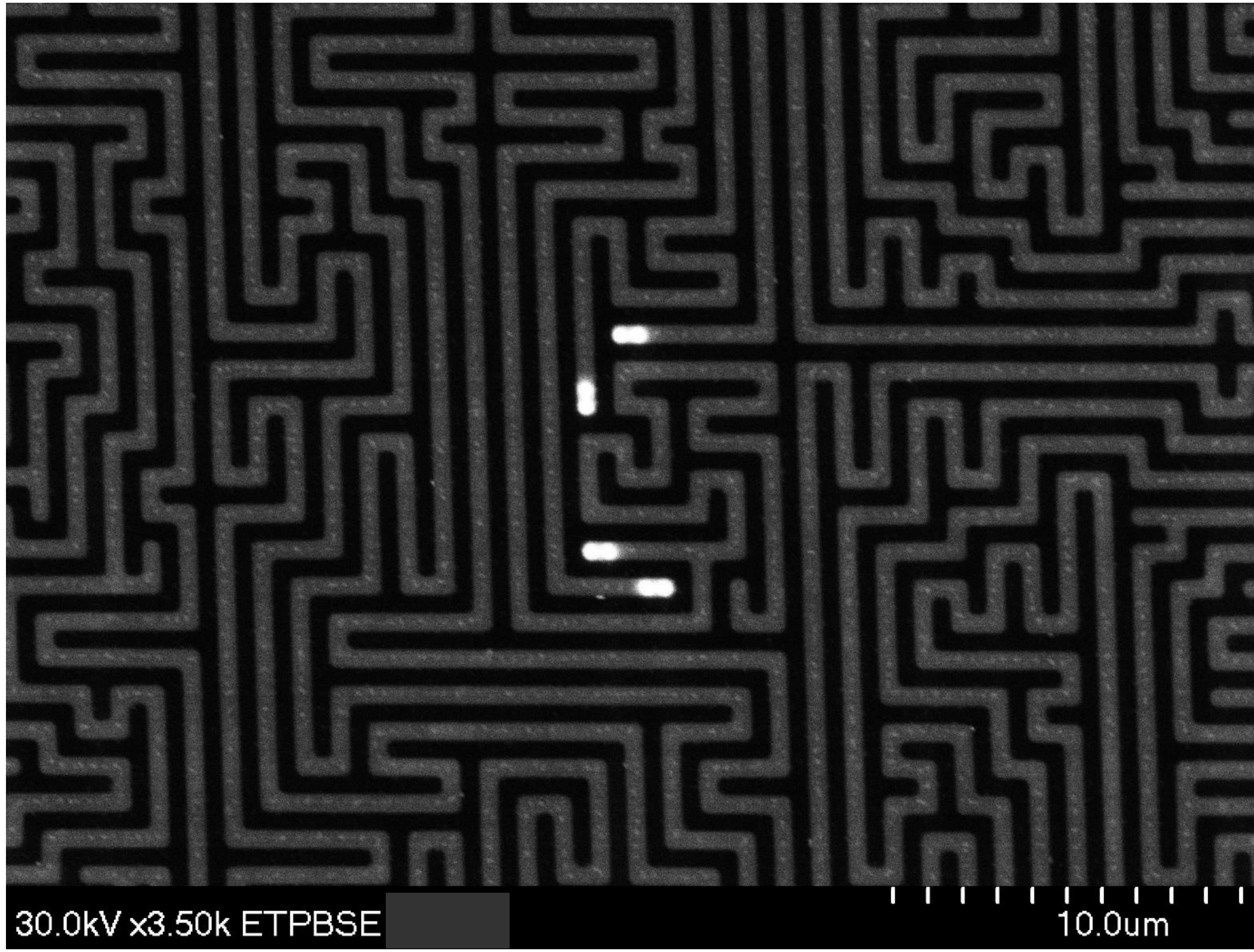
- Is this useful?
- Only a small area removed
- Difficult to align to tracks under shield
- Easy to short-circuit your FIB edit to the bridge created on the shield



First find the contacts

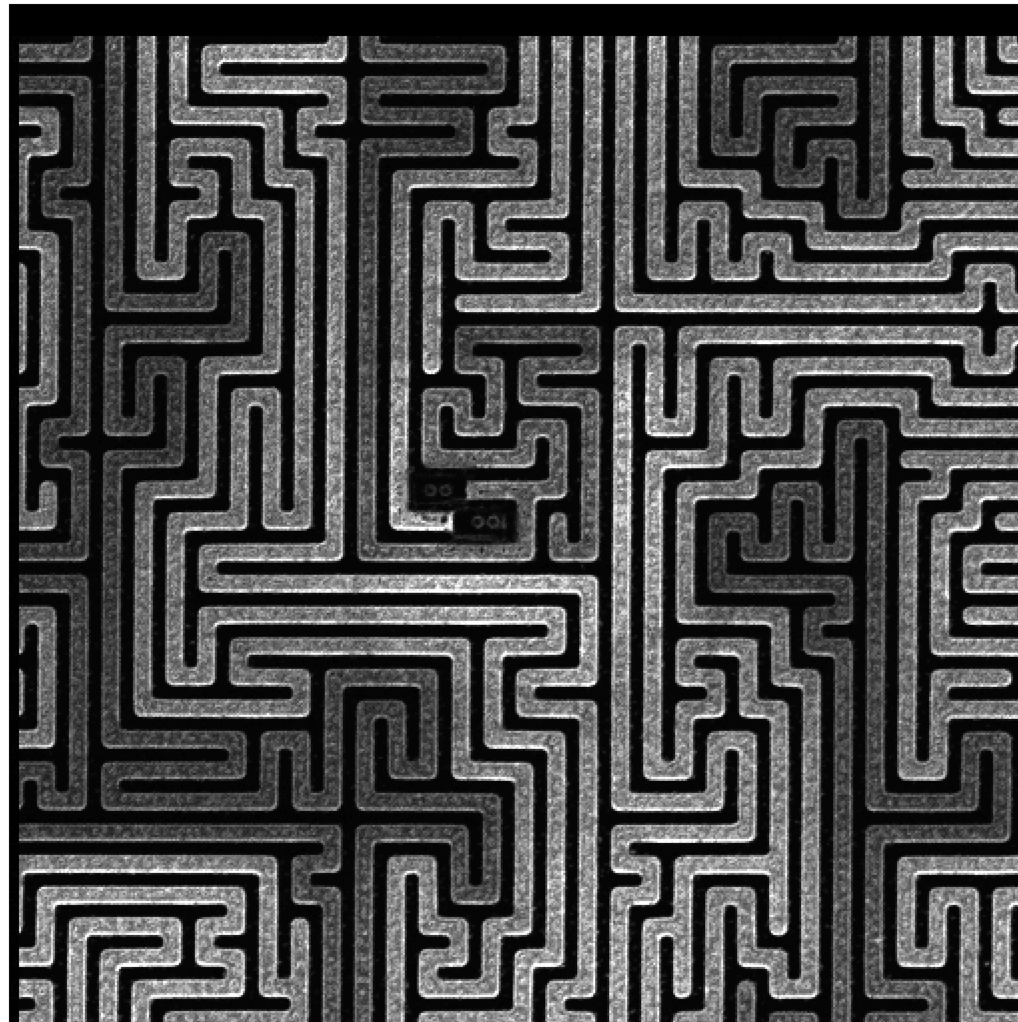
Use backscattered electrons to look for tungsten plugs

- First, find where the tracks contact the circuit below
- Use backscattered electrons to look for tungsten plugs

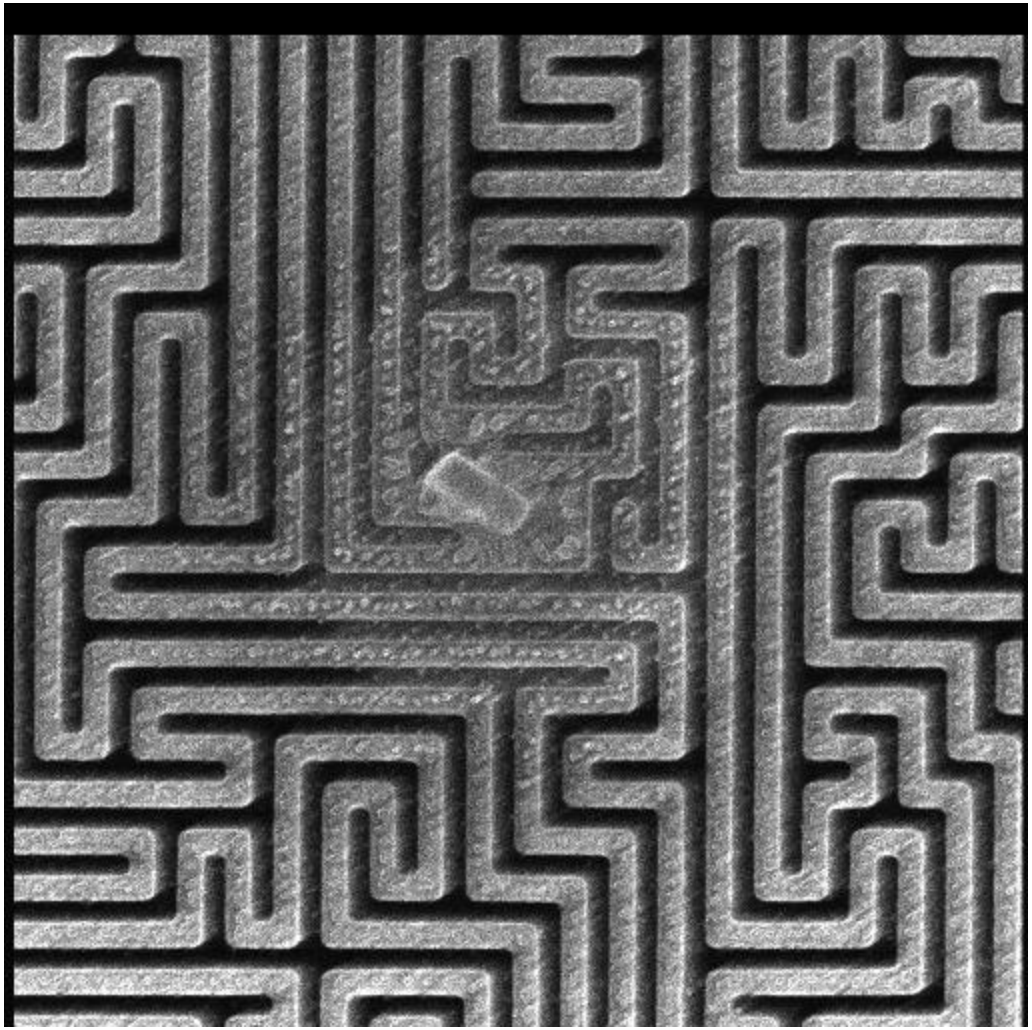


Cut track at each end

- When the track is cut at each end, the track appears dark
- This is a voltage contrast effect



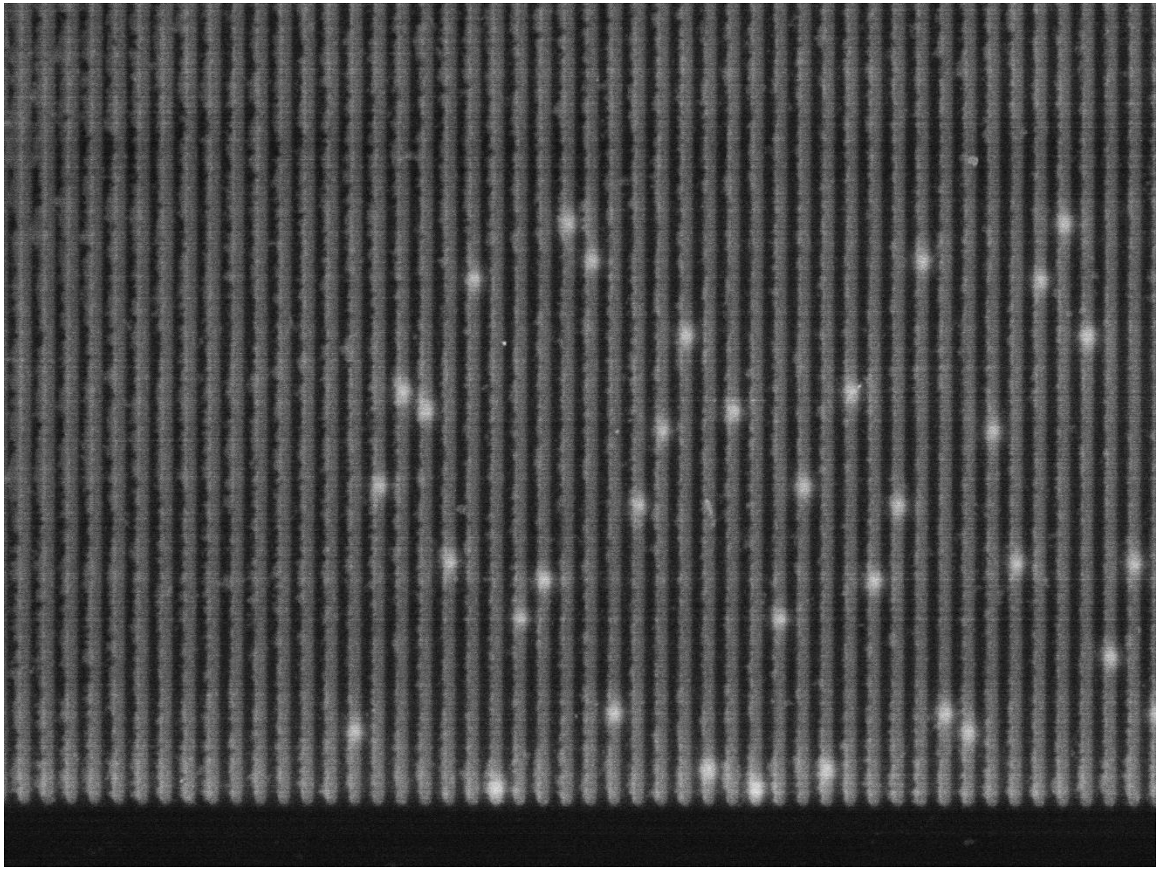
Track ends are short-circuited



Shields with parallel lines

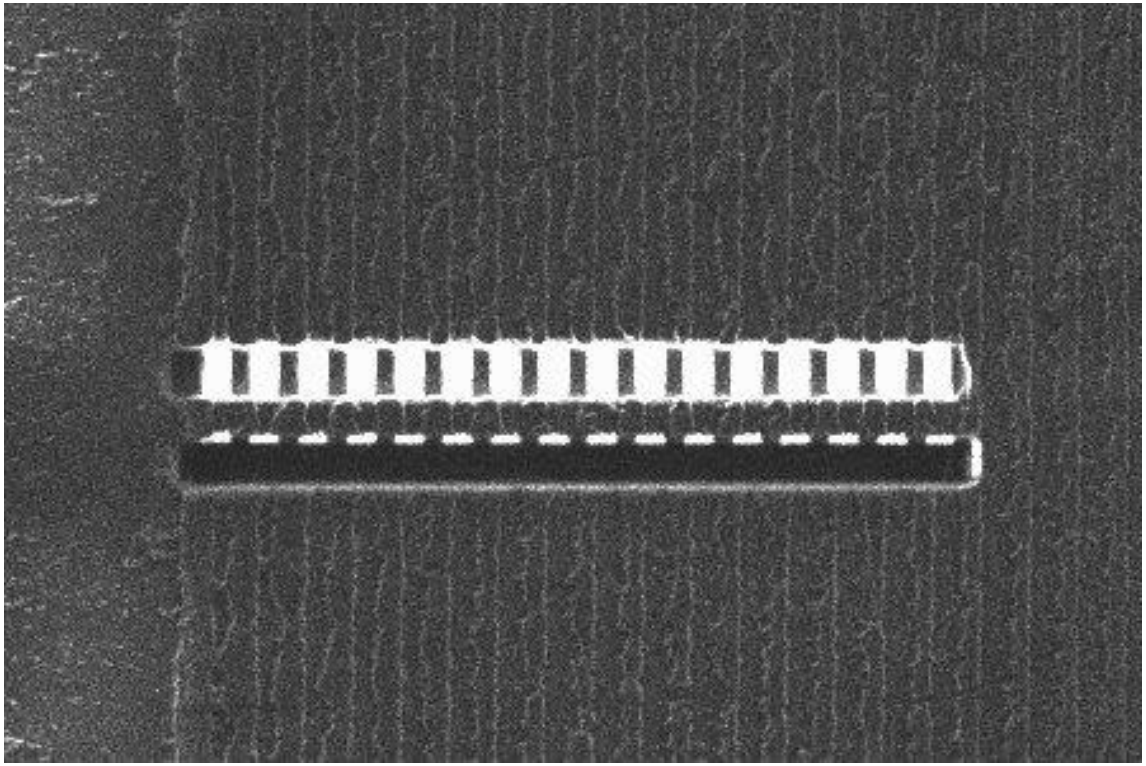
Use backscattered electrons to look for tungsten plugs

- First, find where the tracks contact the circuit below
- Use backscattered electrons to look for tungsten plugs

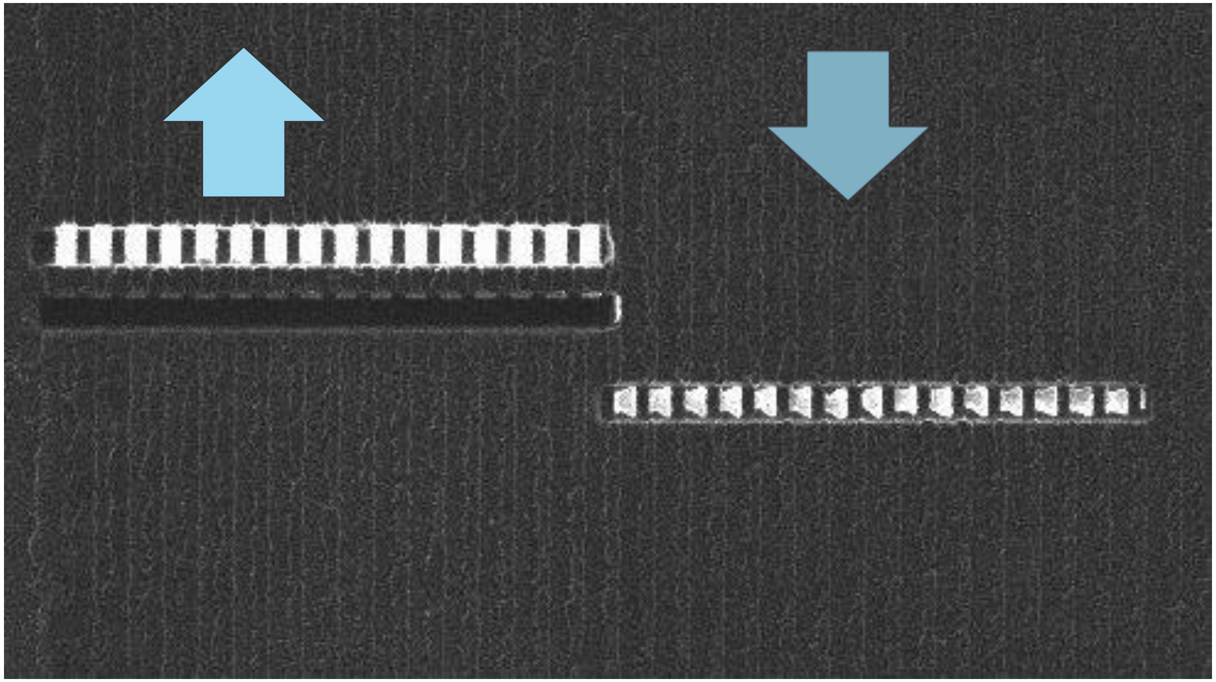


Use voltage contrast to find connections

- First, try to map out the basic shield structure
- Expose the sixteen separate shield lines
- Cut the lines close to the contacts below

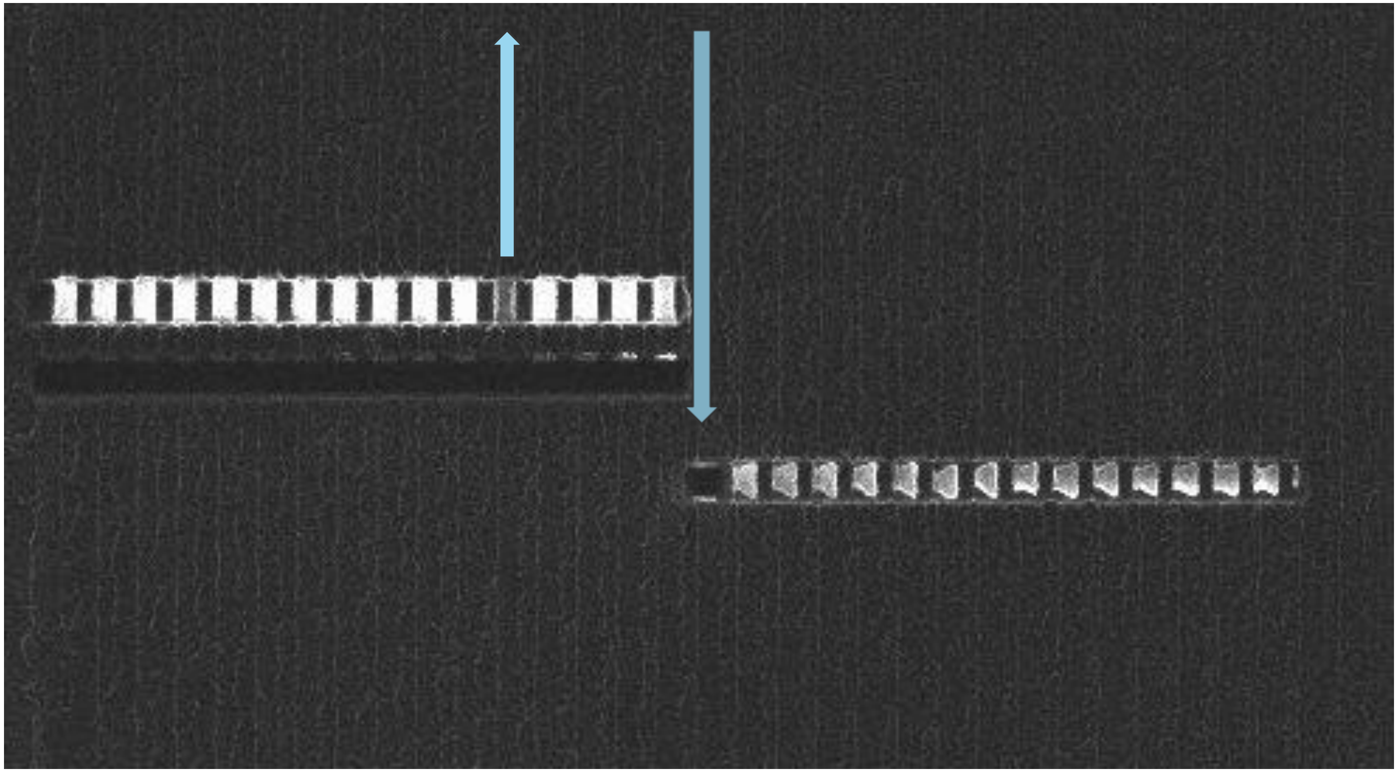


- Expose the circuit lines of the second column of contacts



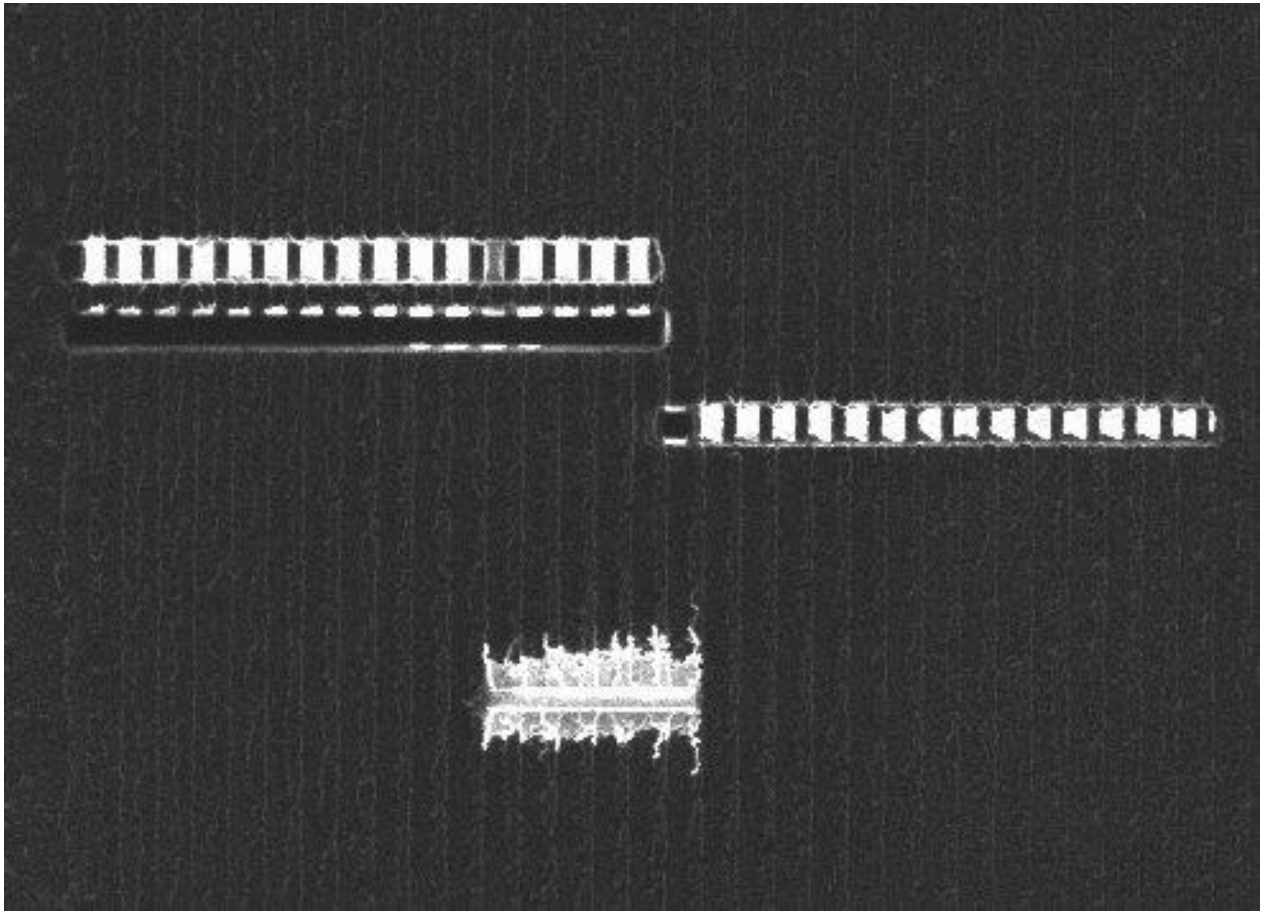
Cut the first track

- Cut one of the lines of the second column
- Note which line goes dark (voltage contrast)



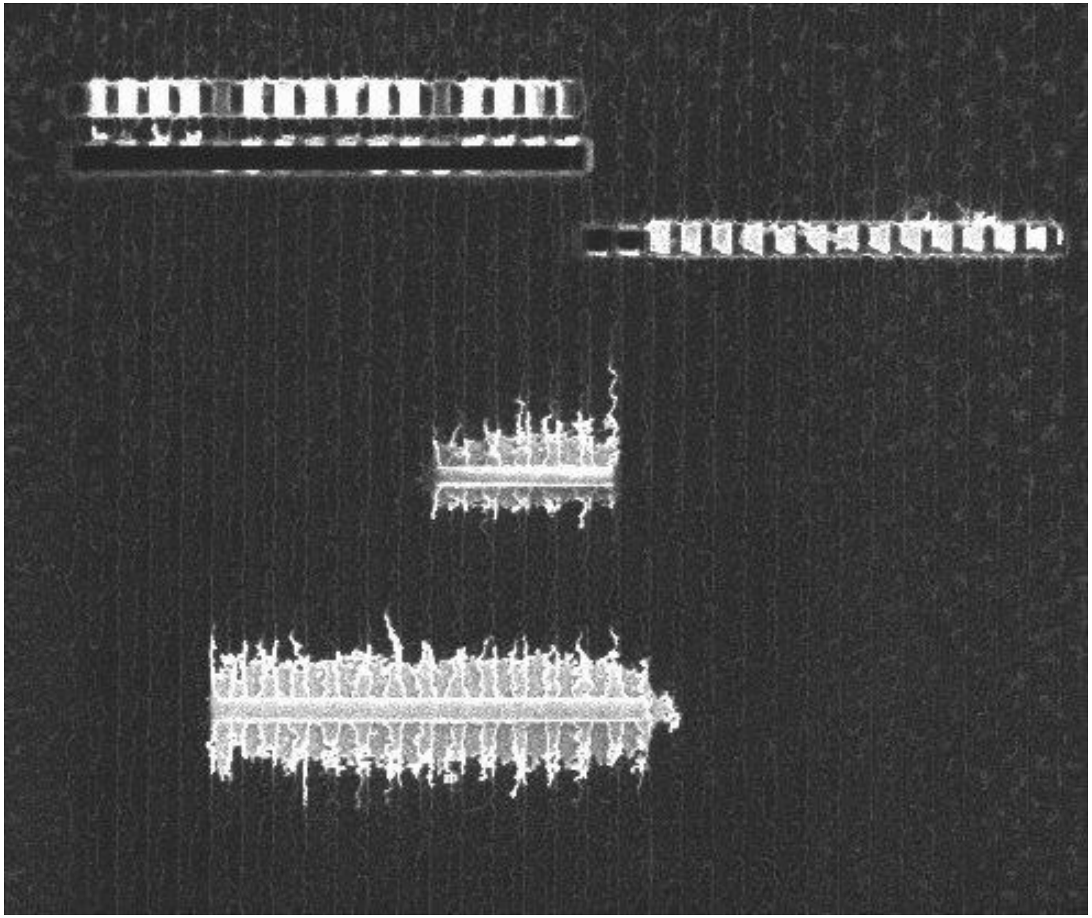
Restore the shield

- Connect the lines of the chosen track to bypass



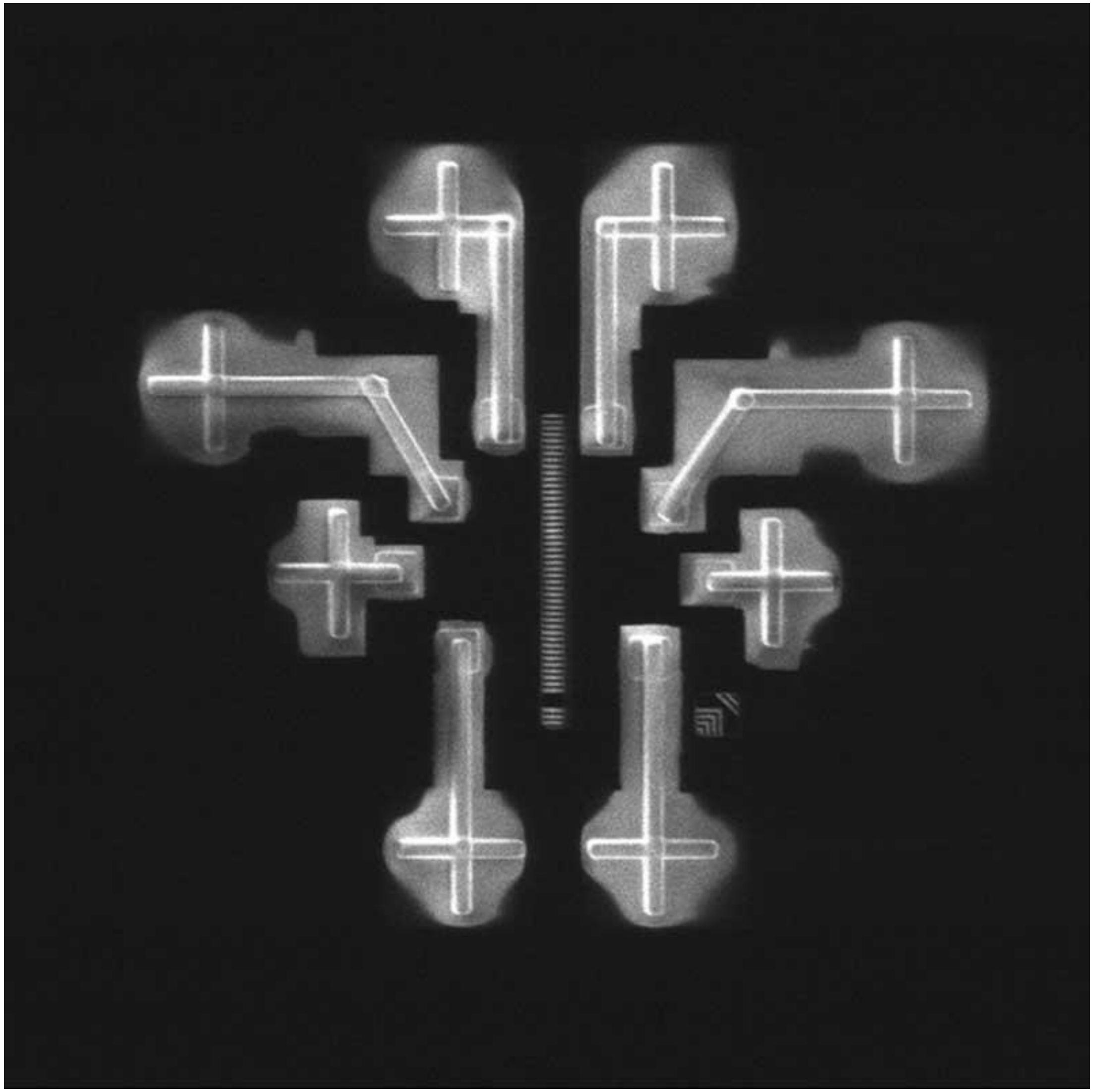
Continue to cut shield and restore

- Connect the other lines to bypass the whole circuit block



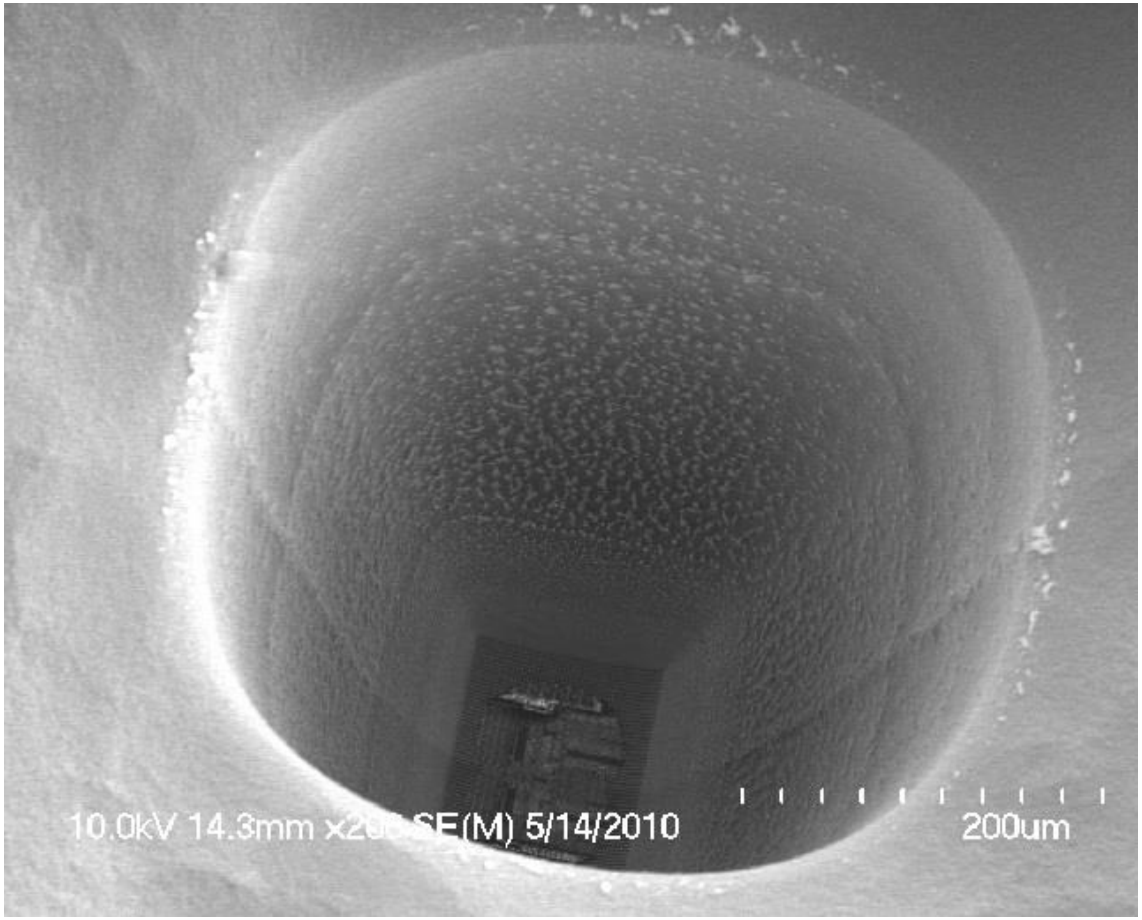
Data gathering with internal probing

- Placing probe points on a bus
- Disable RNG and RNG checking
- Enable JTAG
- Read or set registers



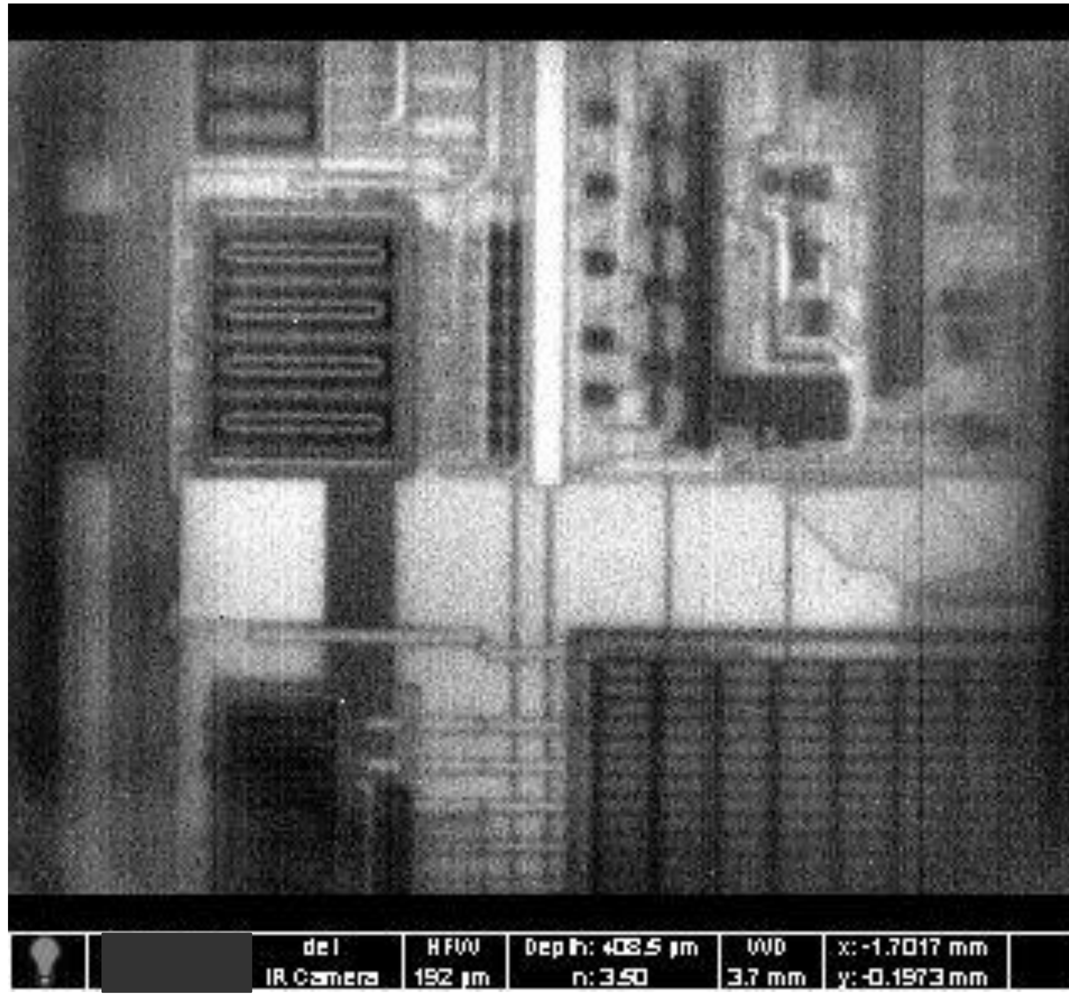
An alternative route to the data: backside edit

- If the active shield is too hard to bypass
- If it is a flip-chip with ball bonds
- If the interesting tracks are really deep

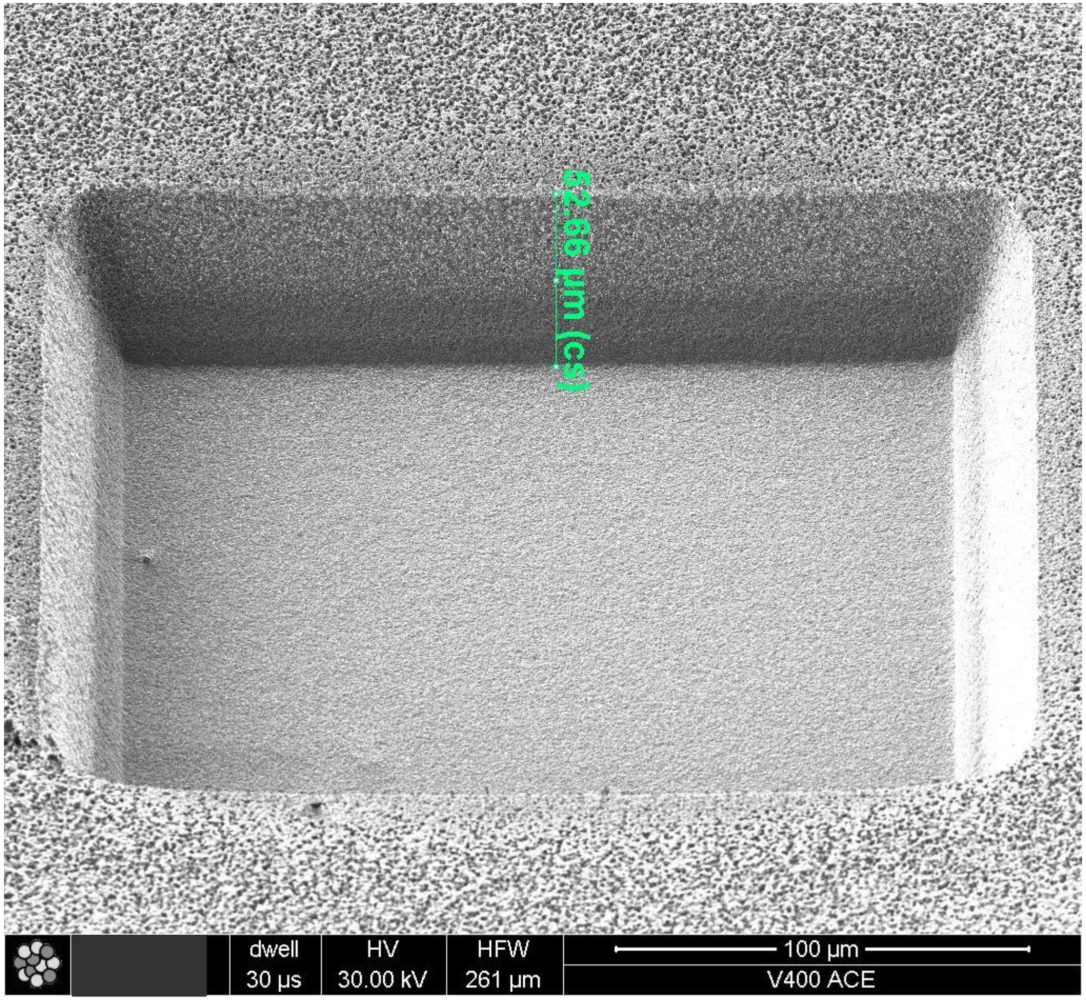


Find your feature – IR microscopy

- Backside edit uses IR microscopy to find an area of interest
- IR resolution is about 1µm. Small tracks cannot be seen
- You need to have an accurate reverse engineered layout and nearby alignment points
- You should also know where the n-wells and other implanted areas are. Very hard for hackers without the GDS11 layout



Start digging

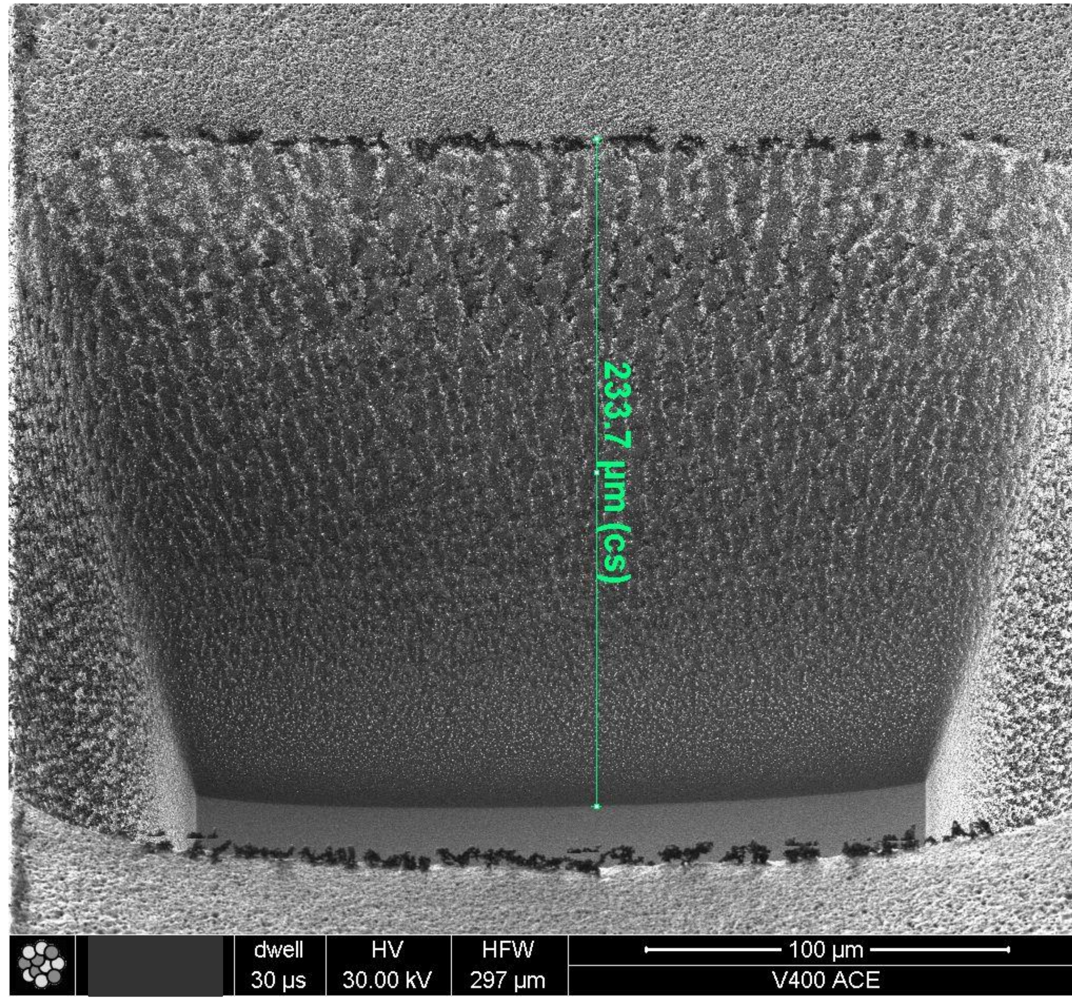


Hardware.io

The Hague, Netherlands

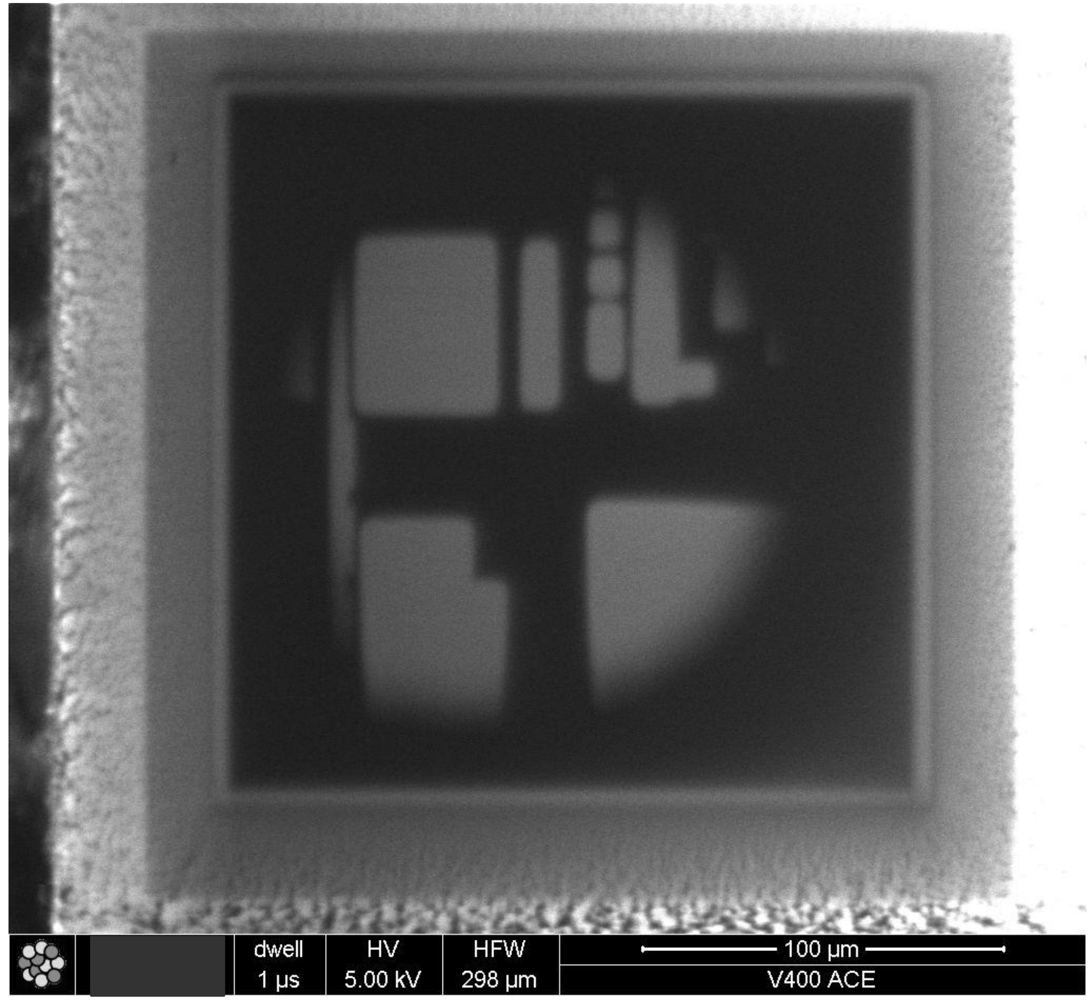
September 2019

Keep digging



Stop digging

- N-wells become visible
- Stop digging immediately
- Align to layout points between active areas
- Cut tracks, join tracks or put down probe points (and hope you can reach them)



Congratulate yourself