Patching hardware remotely: physics vs 0days

11/02/2014

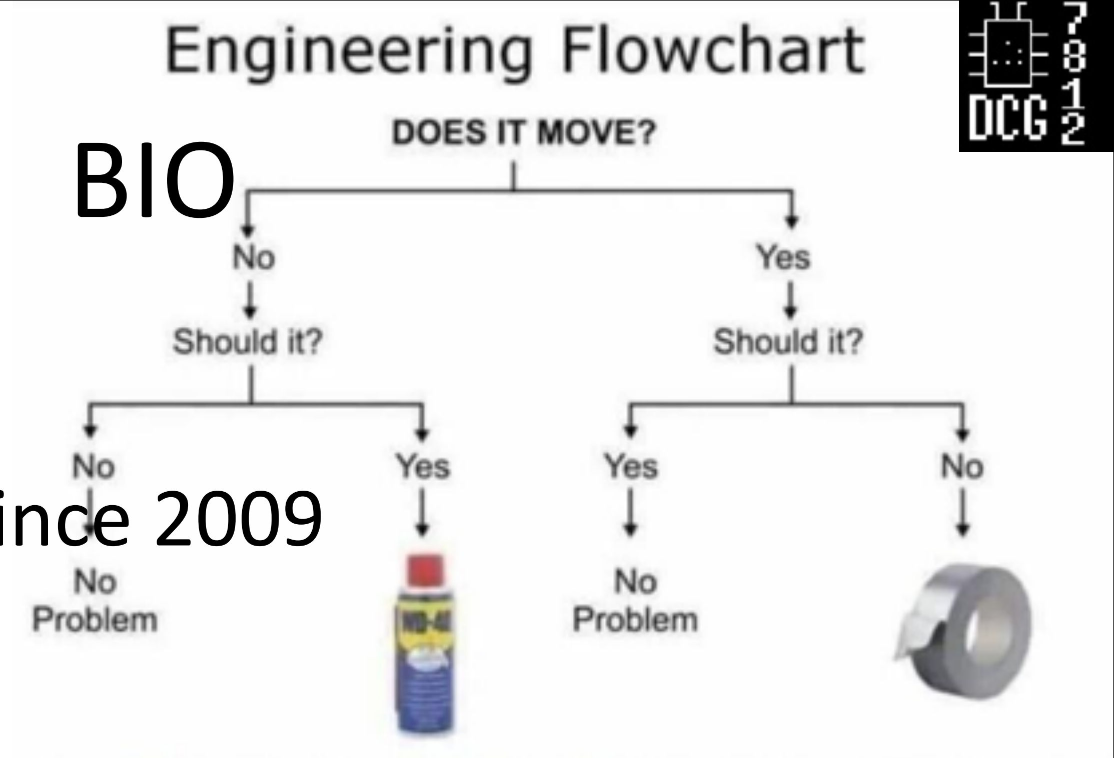
DCG #7812

St.Petersburg

by
@d0znpp

BIO

- physicist
- web app security since 2009
- CEO

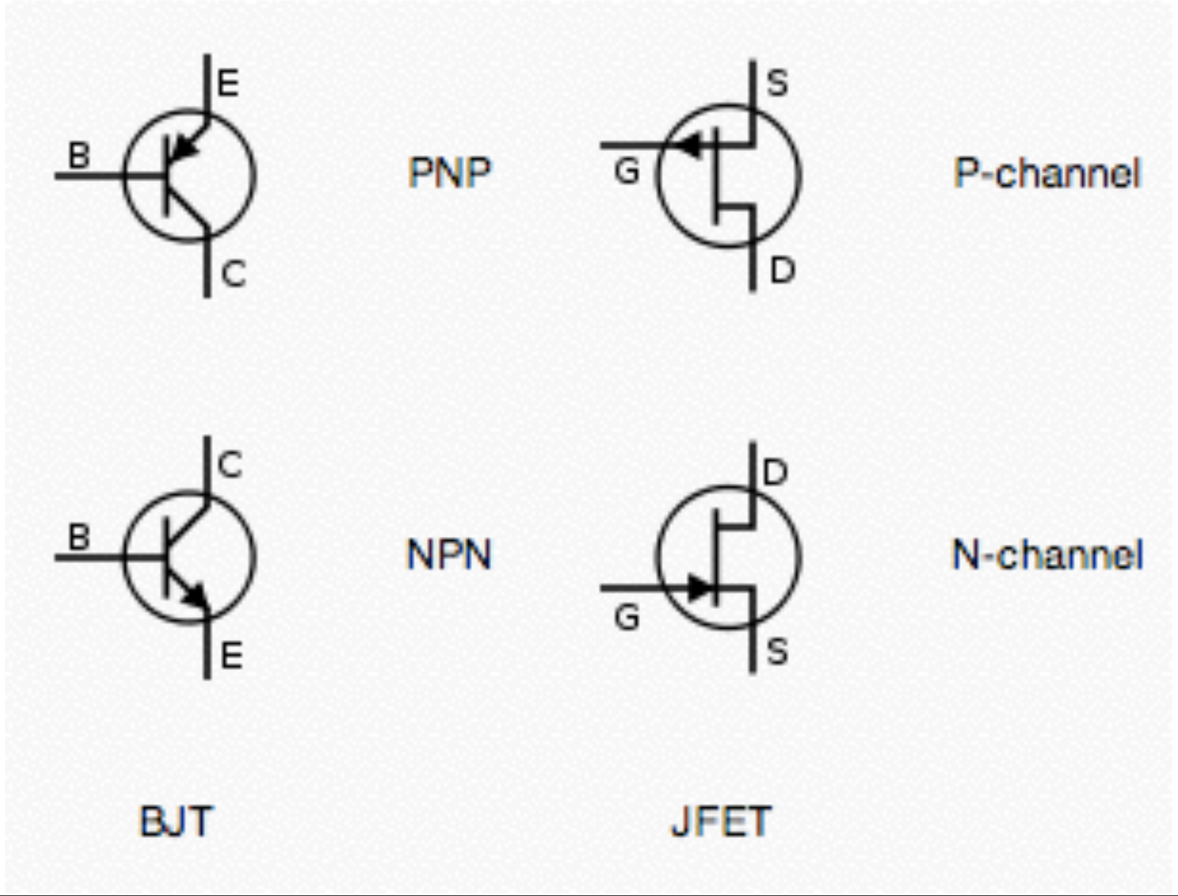


Main question

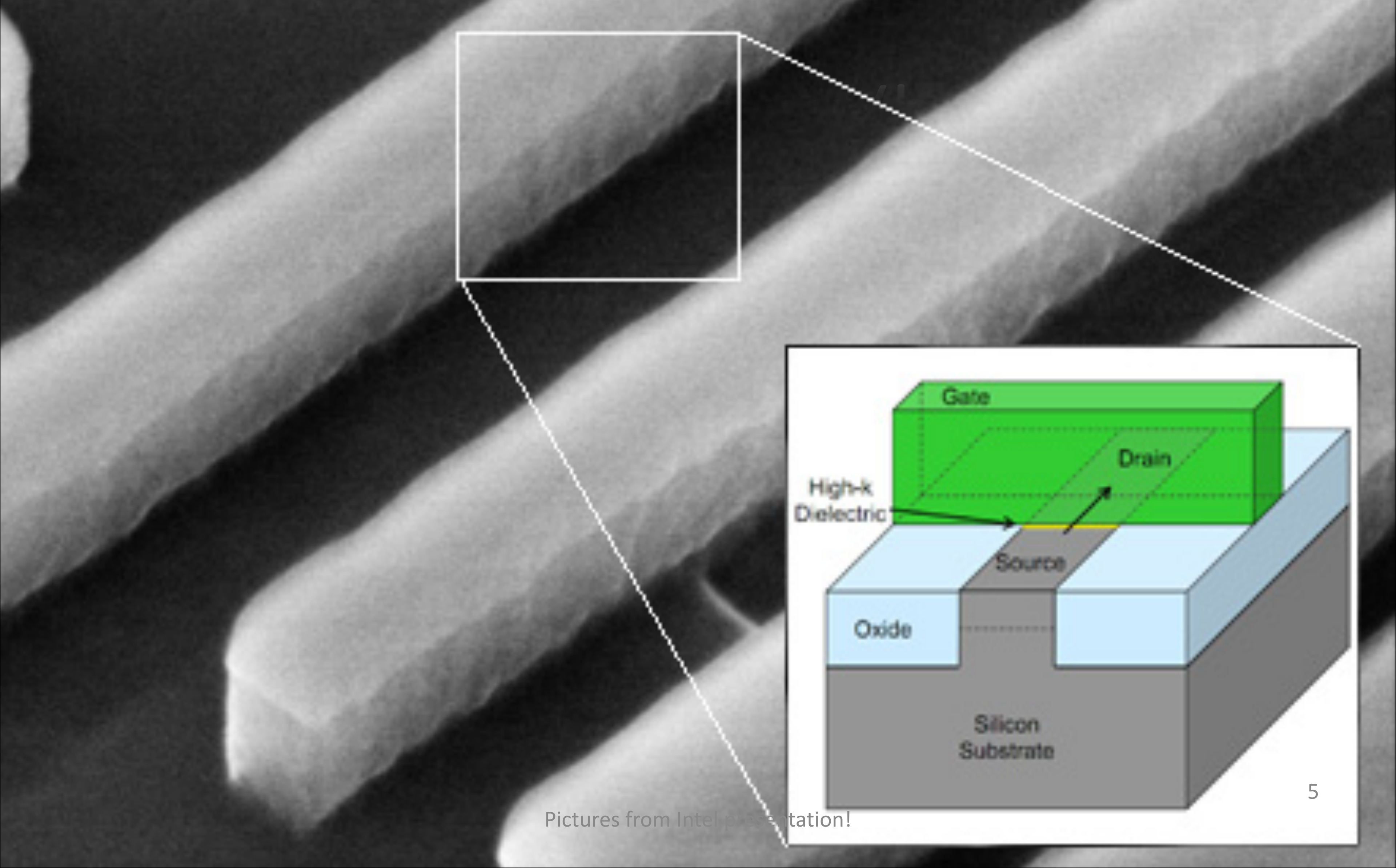
- Is it possible to patch your PC remotely?
- What techniques and tools?
- How much it might cost?
- Physical methods of interaction with semiconductors in distance
- Contactless recording on magnetic storages

Transistors

- 90/60/45/32/22 - well known, yes?
- But what is inside?

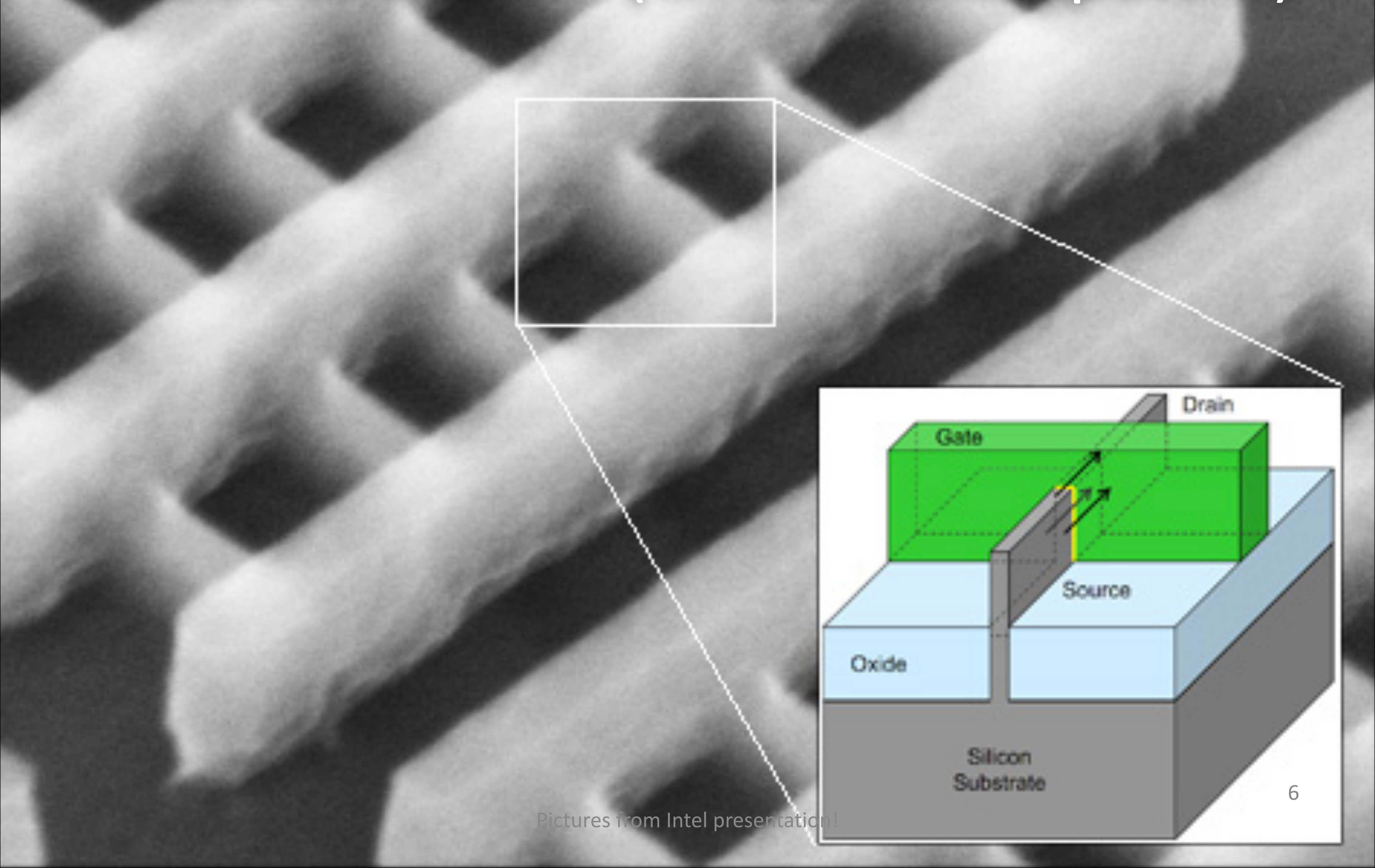


Transistors 32nm (planar)



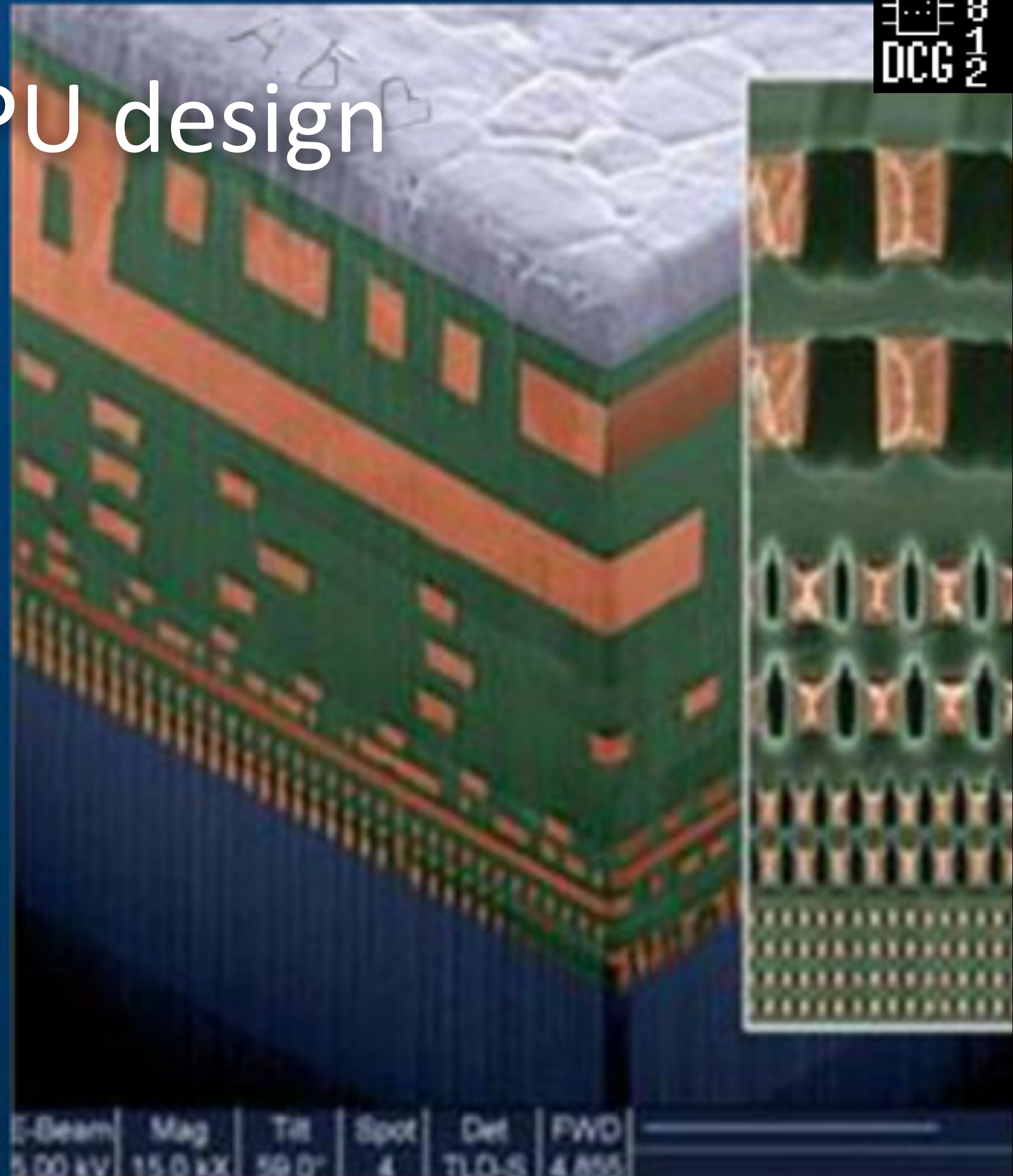
Pictures from Intel presentation!

Transistors 22nm (Tri-Gate Intel patent)



Pictures from Intel presentation!

CPU design



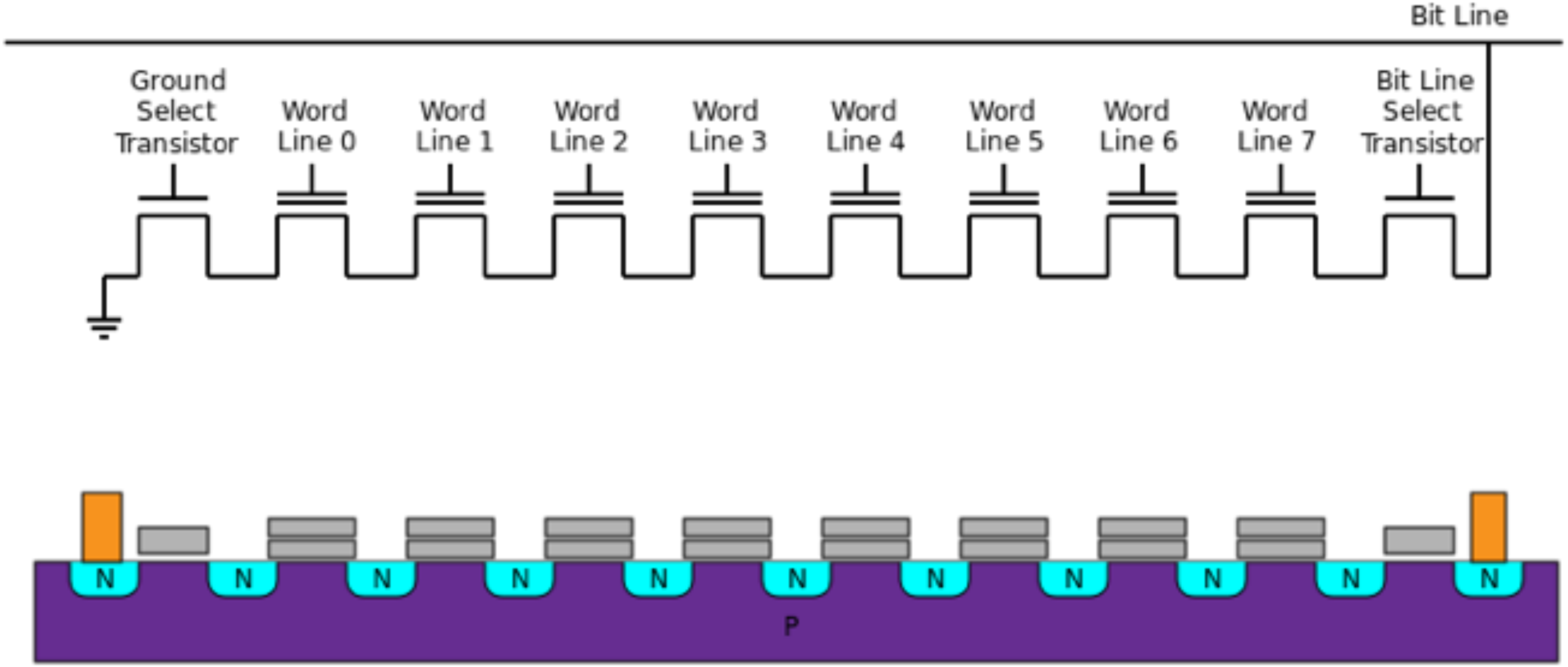
Pictures from Intel presentation!

And what?

- Not information about transistors architecture on a board (logic scheme)
- How organized as a process of calculation
- Which elements are responsible for caching, which for calculation, etc
- Duplication logic

SSD

- NAND, NOR and others. Transistors again!



Interaction

- Passive
  - registration (Hall Sensor and others)
- Active
  - X-Ray
  - Electron-beam Lithography
  - Electron Microscopy

Interaction

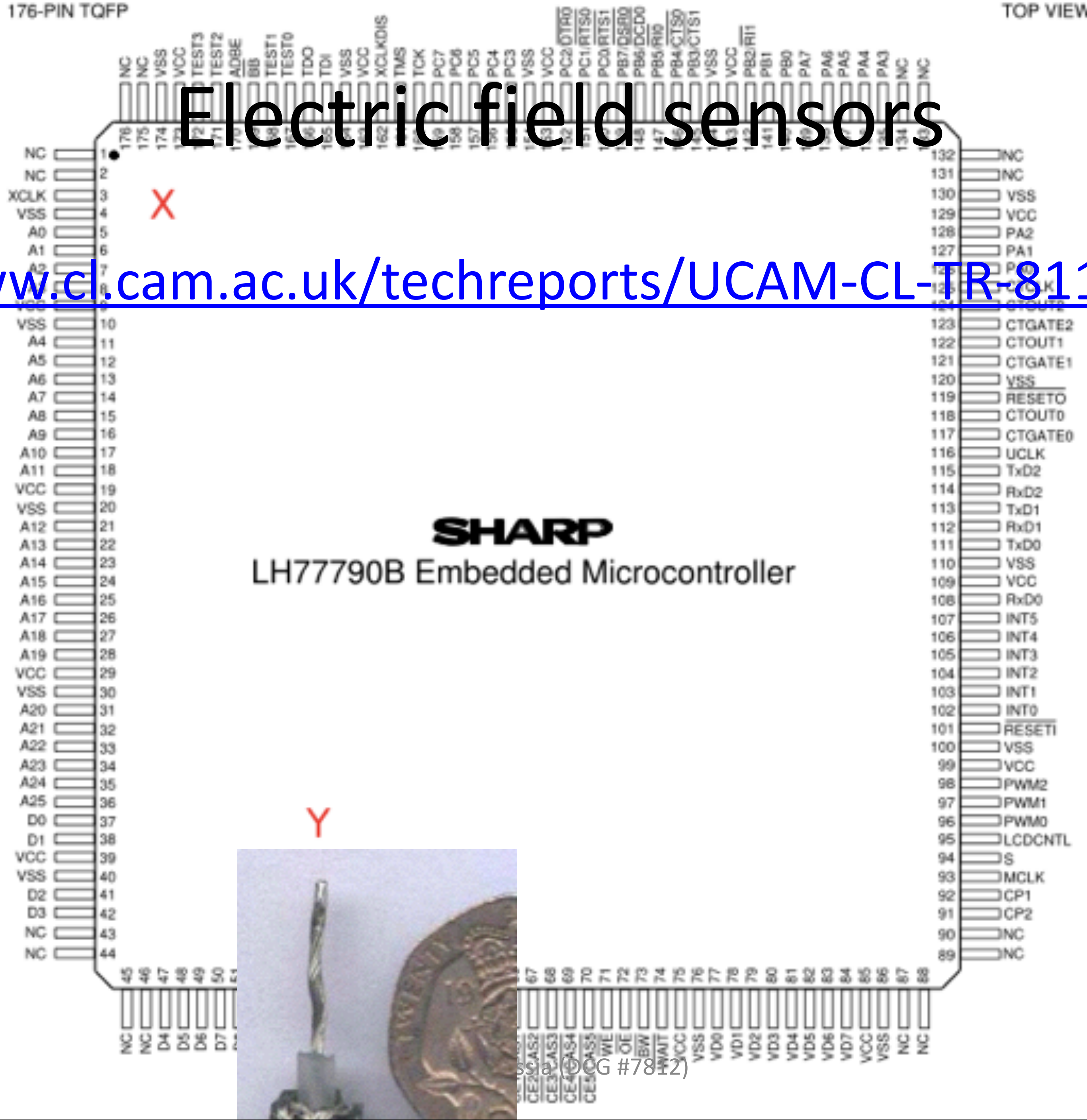
- Passive
  - registration (Hall Sensor and others)
- Active
  - X-Ray
  - Electron-beam Lithography
  - Electron Microscopy

Remote debugging

Remote patching

Electric field sensors

www.cl.cam.ac.uk/techreports/UCAM-CL-TR-811.pdf



Electric field sensor

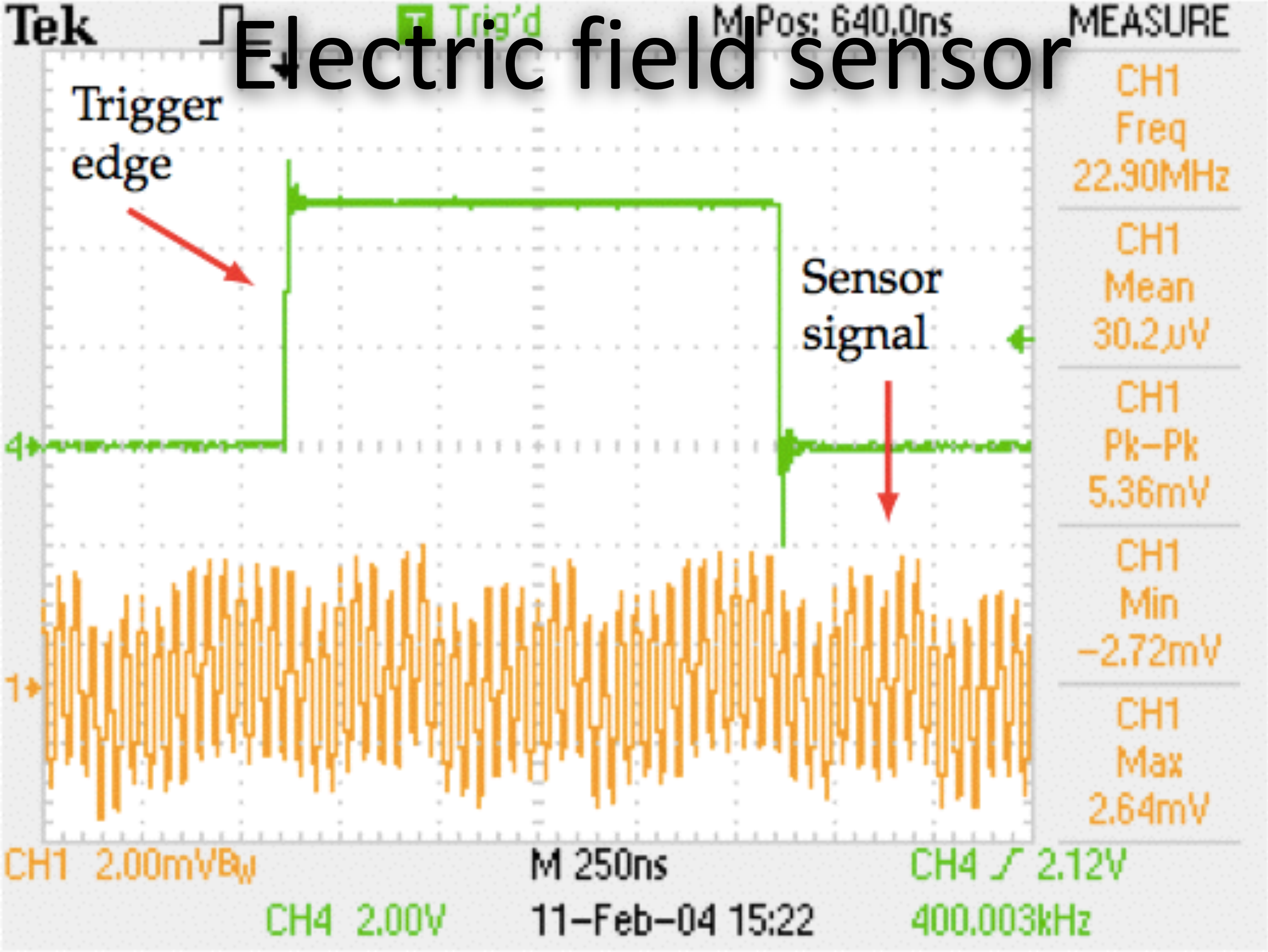


Figure 4.3: *End of half-wave dipole on LH77790B case orientation spot, near XCLK pin (marked as X on Figure 4.2 on the facing page). Appears to be detecting the 25 MHz clock frequency.*

Electric field sensor

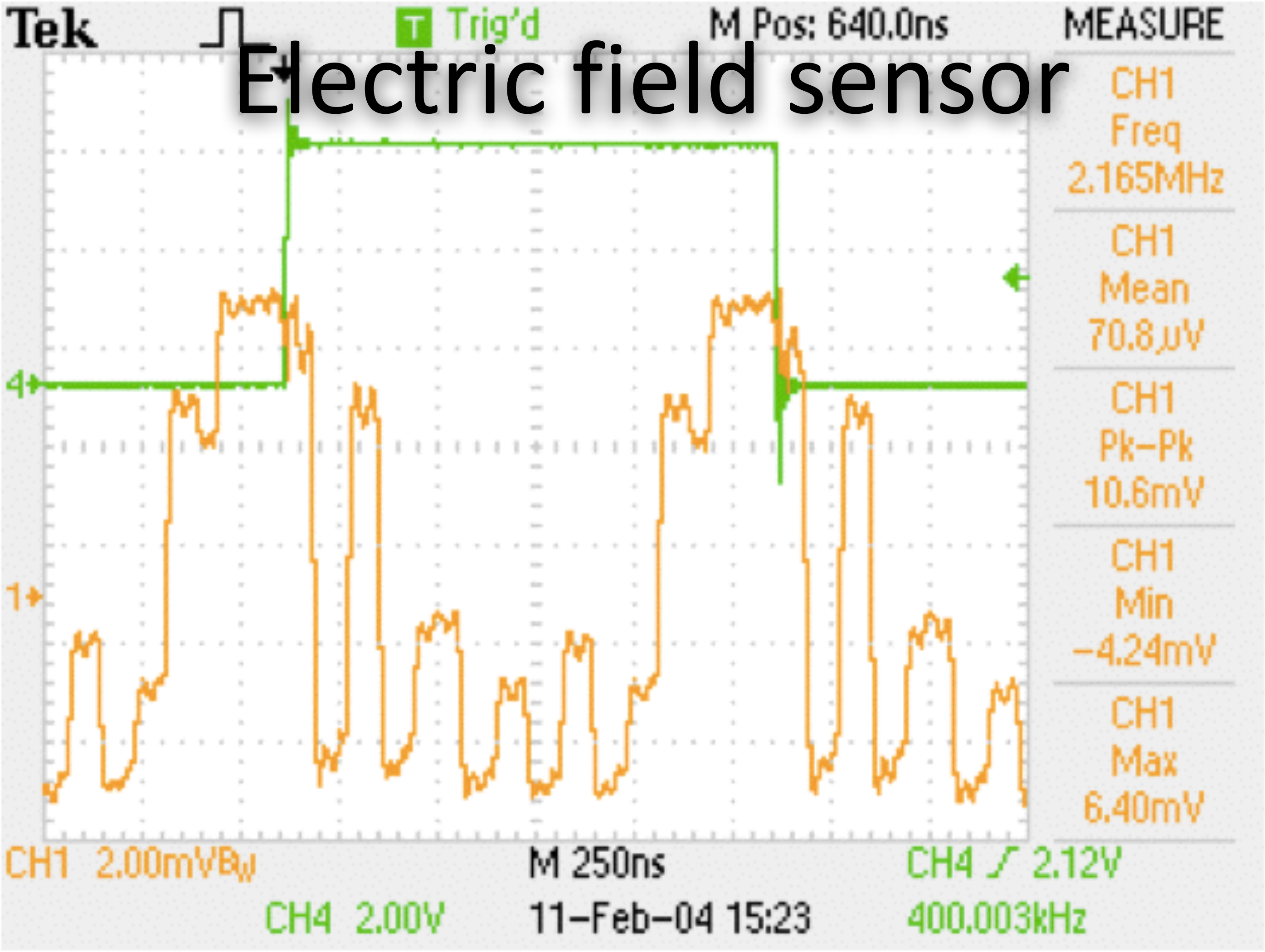
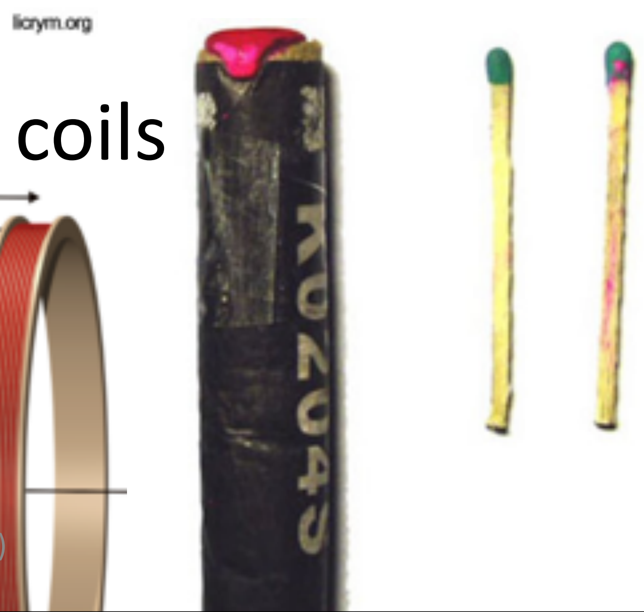


Figure 4.4: *End of half-wave dipole 5 mm in from LH77790B pin 55 (data bus area), marked as Y on Figure 4.2 on page 80. As would be expected, the trace shows much more variation.*

Home-made field source

- Piezo lighter

- Firecracker and Helmholtz coils



Electron lithography

http://pubs.acs.org/doi/abs/10.1021/nl101055h

- «Vacuum-Free Self-Powered Parallel Electron Lithography with Sub-35-nm Resolution»

X-Ray

http://www.icdd.com/resources/axa/vol43/v43_056.pdf

- The Modification of TXRF-Method by Use of X-ray Slitless Collimator
- Up to 30 nm now and 10 nm at future

X-Ray

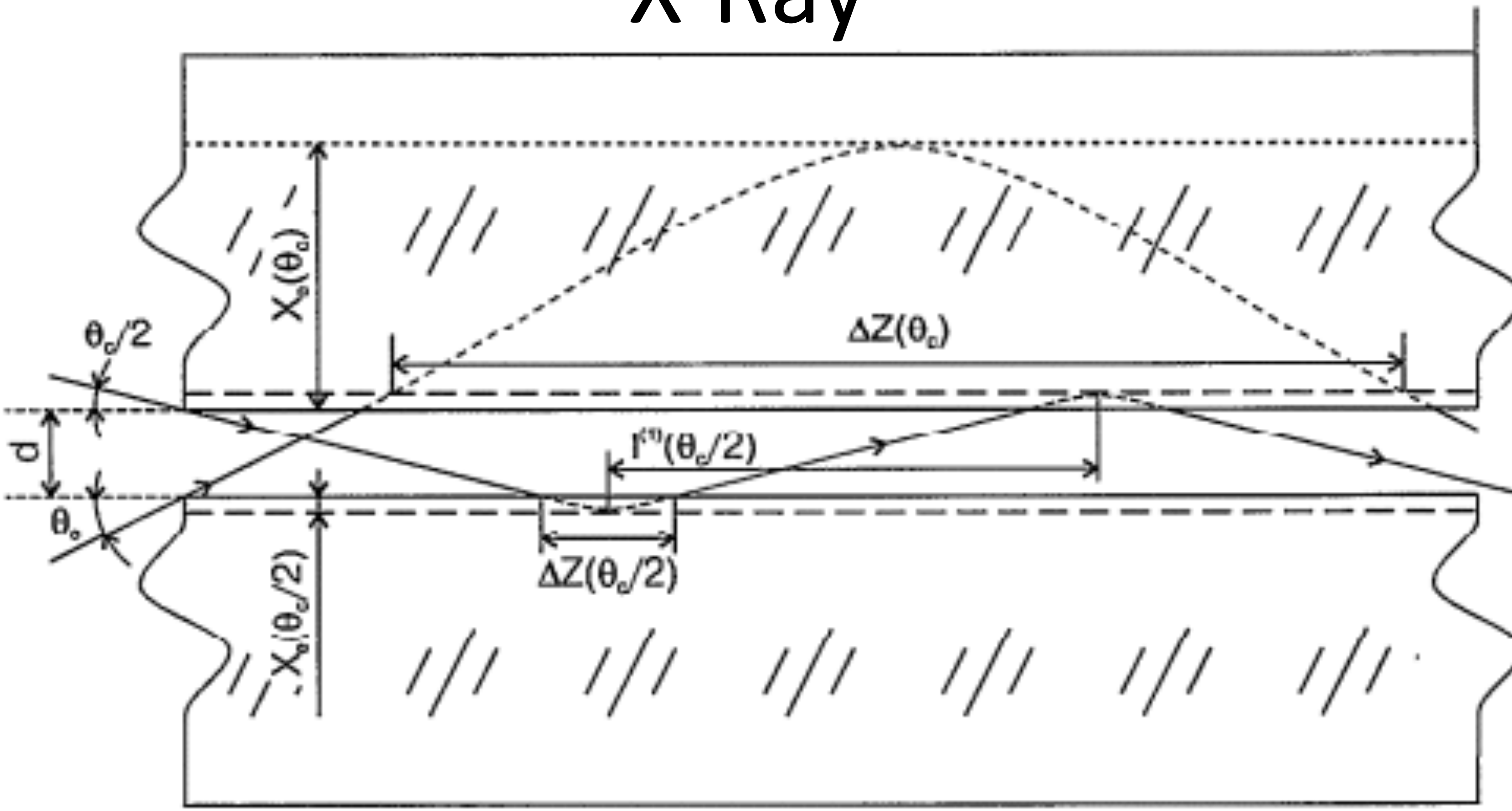


Figure 2. Scheme of reflections for partial X-ray beams entered into the clearance between the quartz plates formed the slitless collimator under θ_c and $\theta_c/2$ angles. Angles are increased for clearly.

Conclusion

- Modern CPU and other devices has no protection from active and passive electromagnetic interactions
- It’s possible to create this protection by sputtering (f.e. cathodic)

Next steps

- Collect a lot of CPU
- Cut, spray them and analyze spectrum to determine the exact chemical composition of elements
- Restore the component scheme (block-level data)
- Fuzz using X-Ray (start from registers)