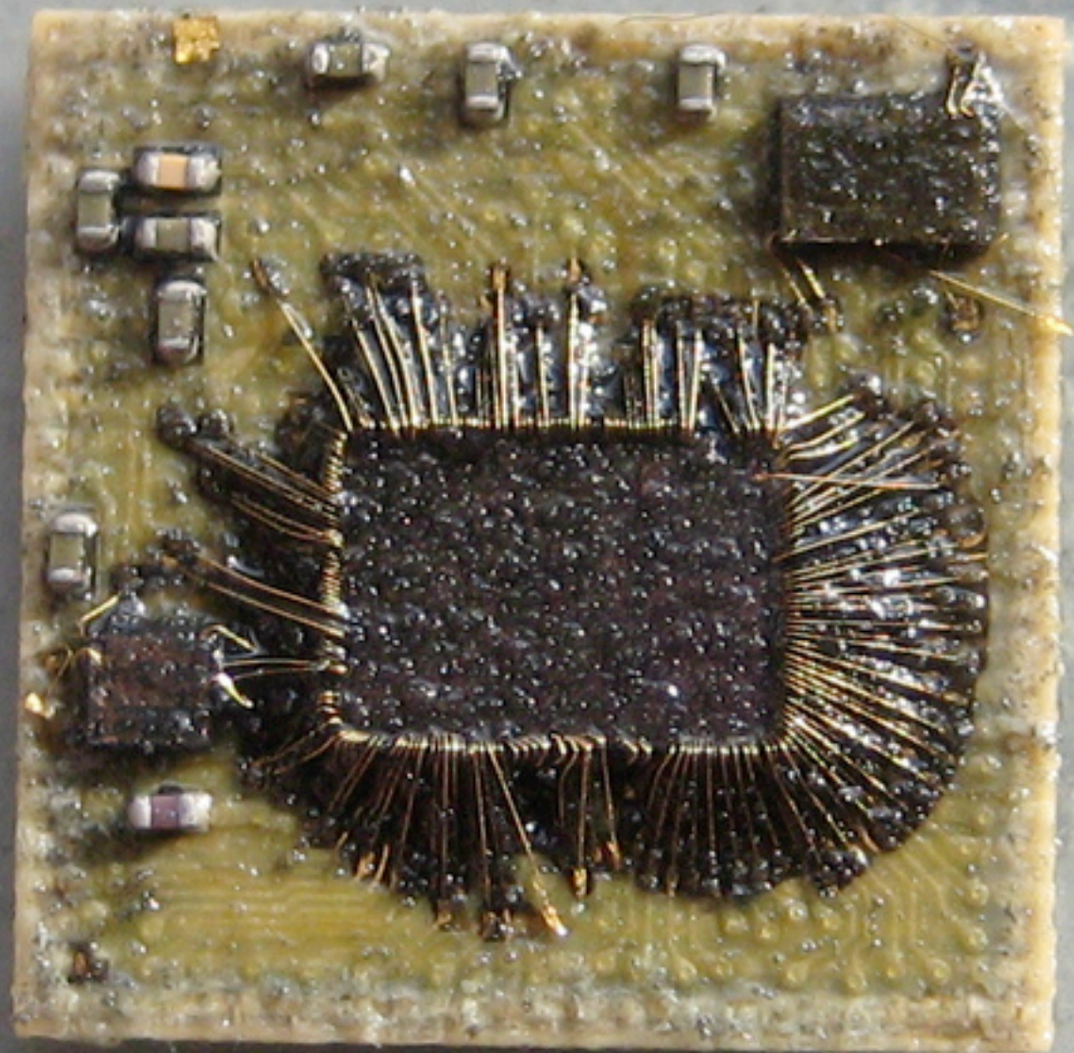
Travis Goodspeed

May 2011, Kraków, Poland



Practical Attacks against the Freescale MC13224 ZigBee SoP

Wednesday, May 25, 2011

Firmware Extraction

- You have a device.
- You want a remote exploit, keys, whatever.
- First you need a copy of the software.
  - Chips can be locked.
  - Unlocking them is the subject of this lecture.

Freescale MC13224

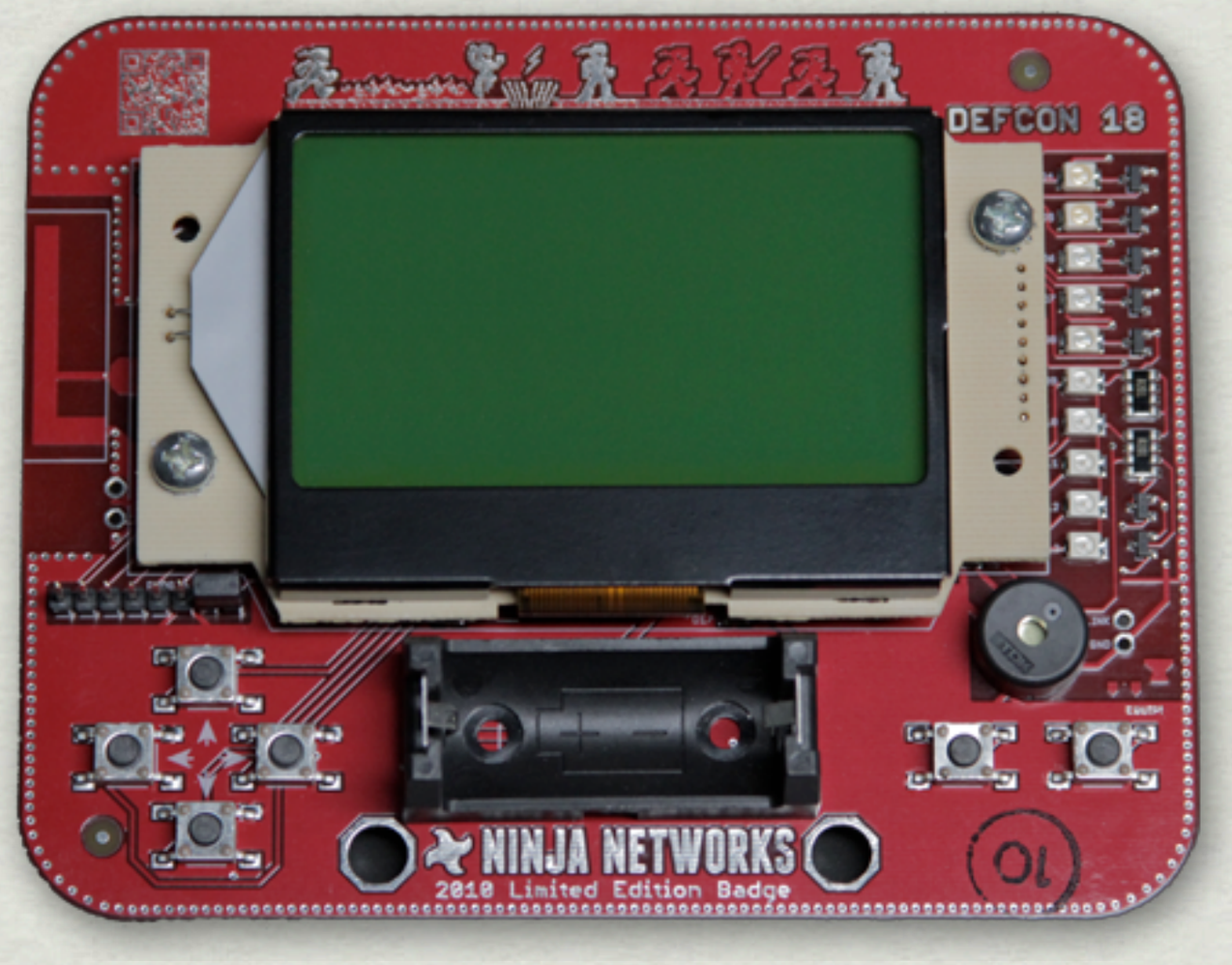
- 128KB Serial Flash
  - Non-executable!
- 96KB of RAM
- 80K ROM
  - Bootloader
  - Device Drivers
- JTAG Debug Port
- AES Accelerator
- 802.15.4 Radio
  - Analog chain in-chip.
  - Easy to design with.
- Lockable flash.

ZigBee / IEEE 802.15.4

- 2.4GHz Wireless Standard
- Not Wifi (802.11) or Bluetooth (802.15.1)
- Becoming common
  - Toys, industrial equipment, etc.

Thank you kindly,

- Babak Javadi
- Mariano Alvira
- Amanda Wozniak
- CStone

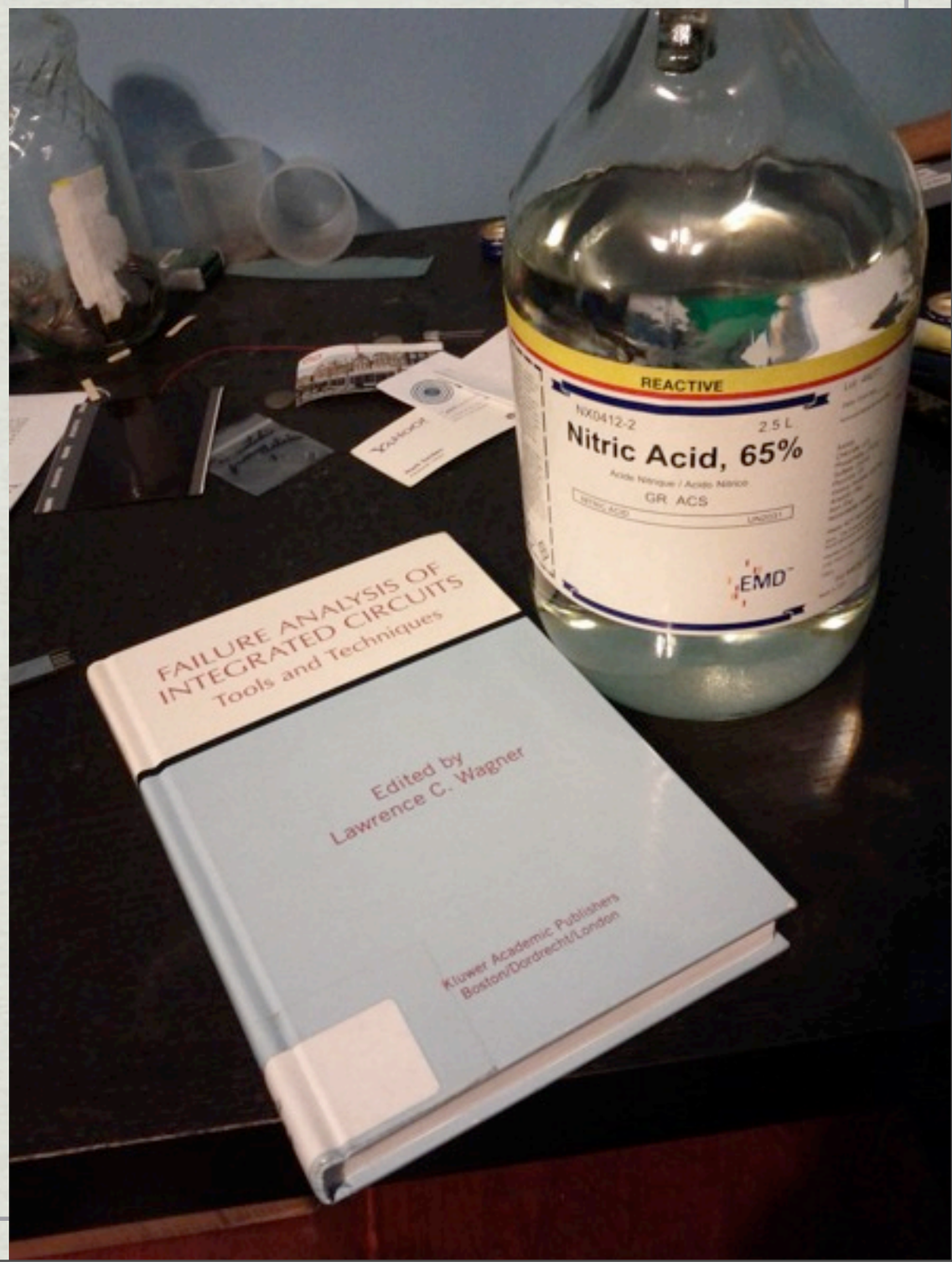


Thank you, Freescale.

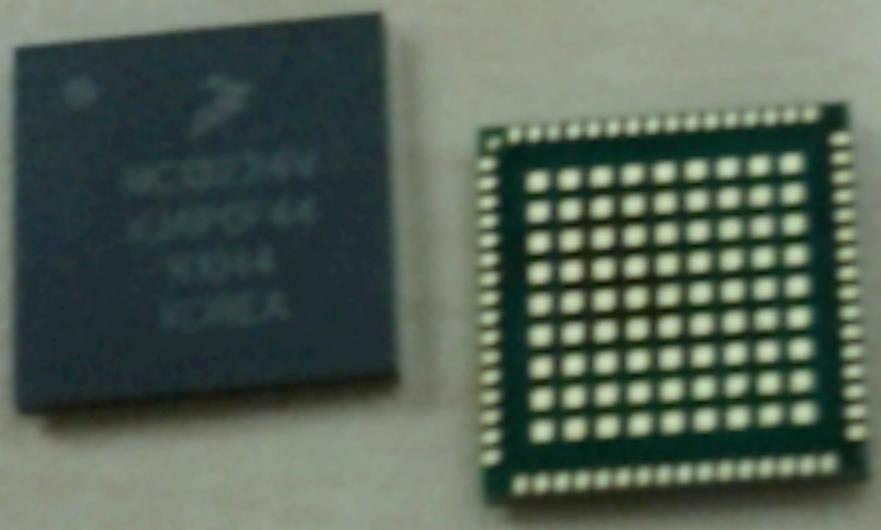
- The MC13224 is a good chip.
  - In-package antenna chain!
- It was never intended to be a smart card.
- It’s harder to build chips than to break them.

Chip Decapsulation

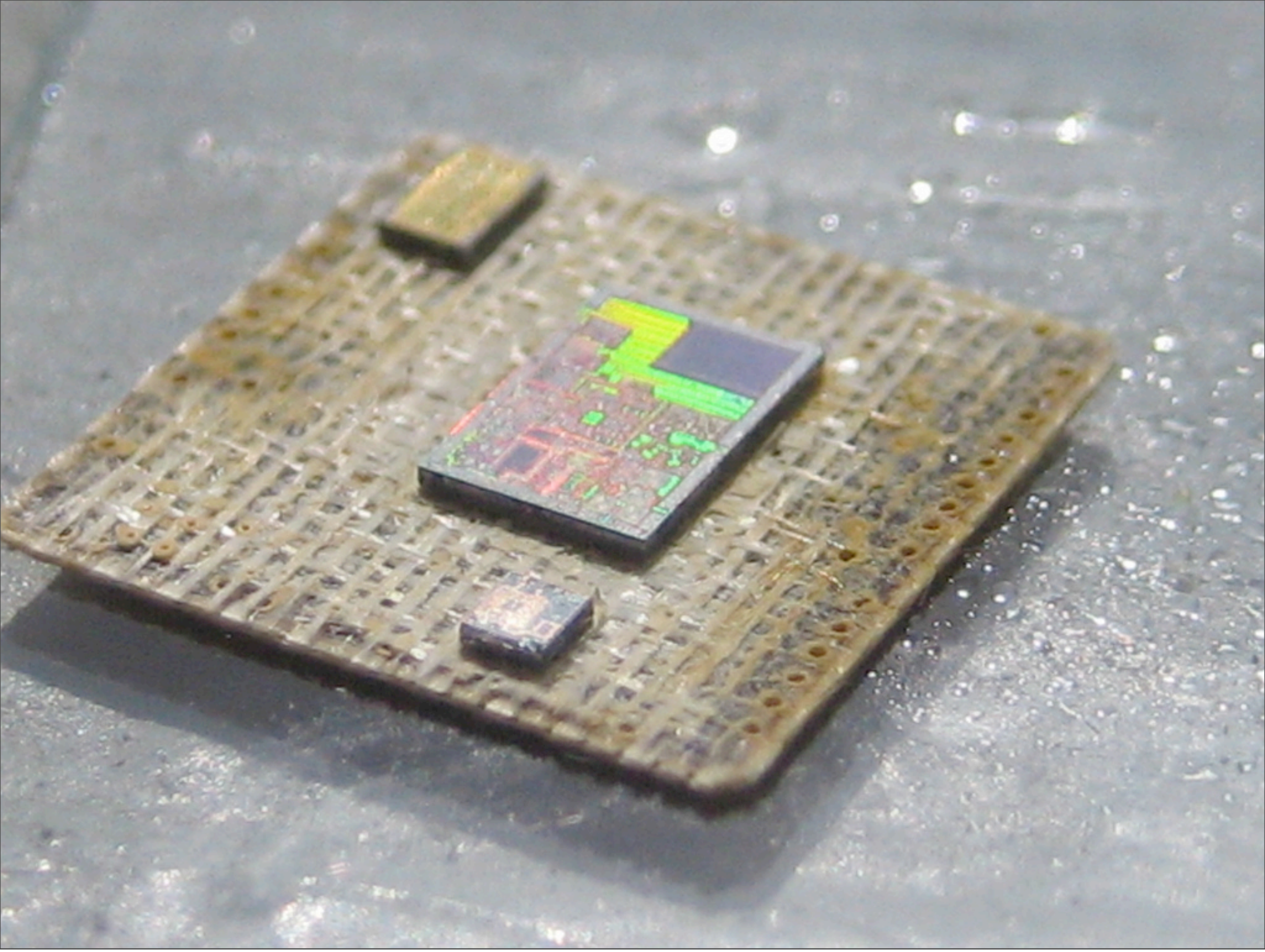
- Nitric Acid (HNO3)
- Sulfuric Acid (H2SO4)

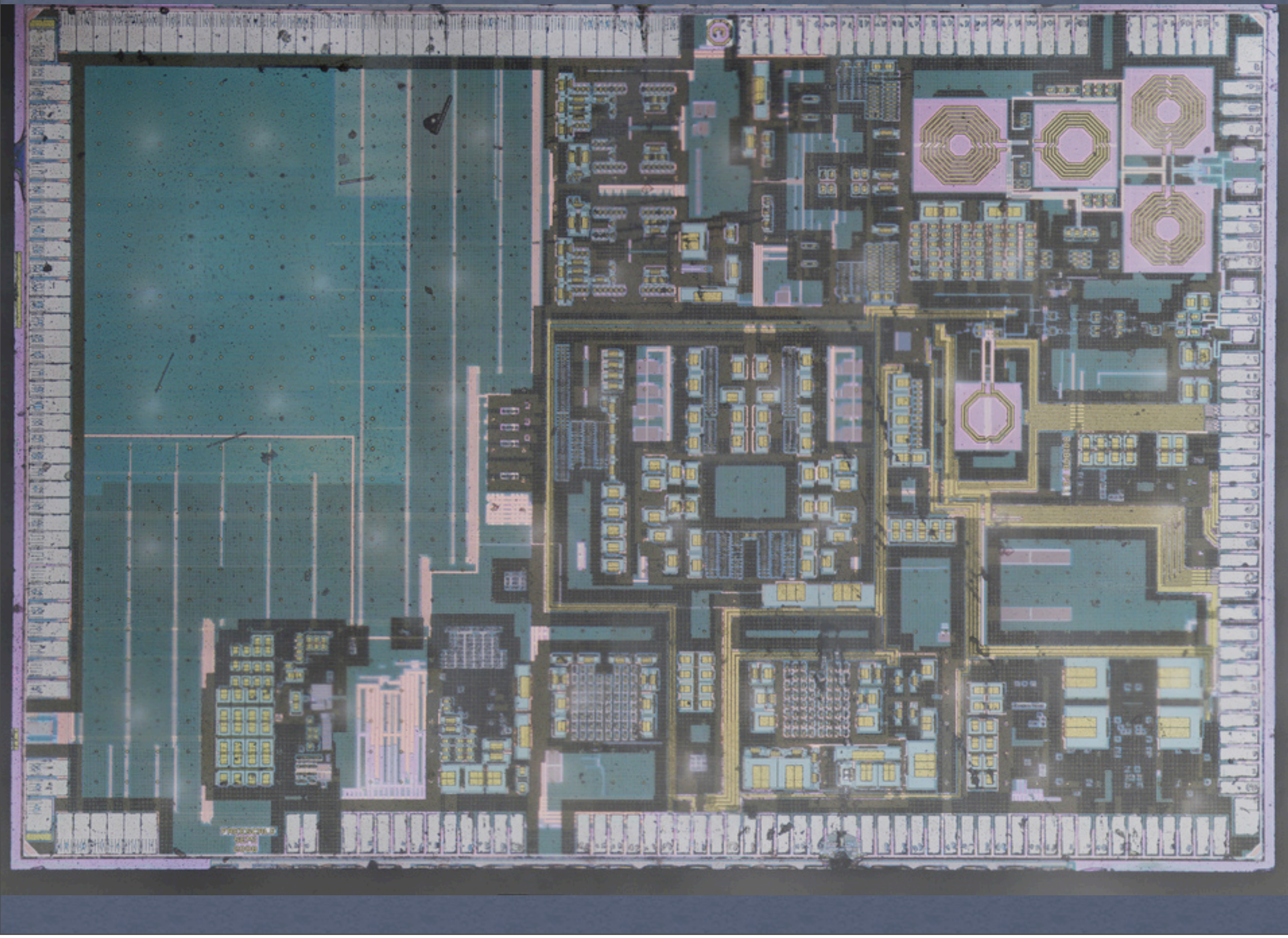


MC13224V



Wednesday, May 25, 2011





How Locking Works

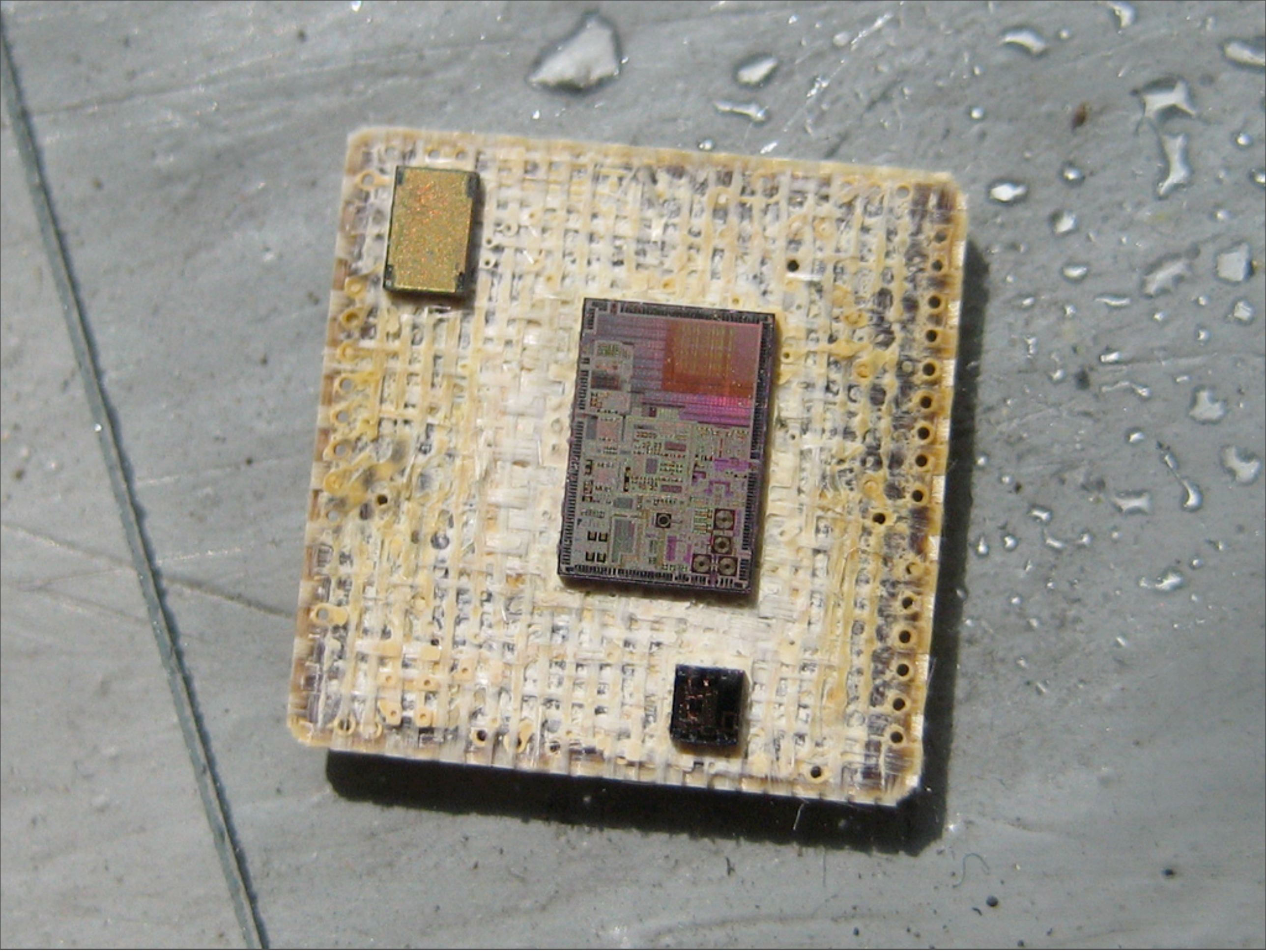
- The chip begins LOCKED.
- The chip looks as FLASH[0:3]
  - “SECU”: Stay locked, boot from Flash.
  - “OKOK”: Unlock, then boot from Flash.
  - else: Unlock, then boot from external memories.

Booting from Flash

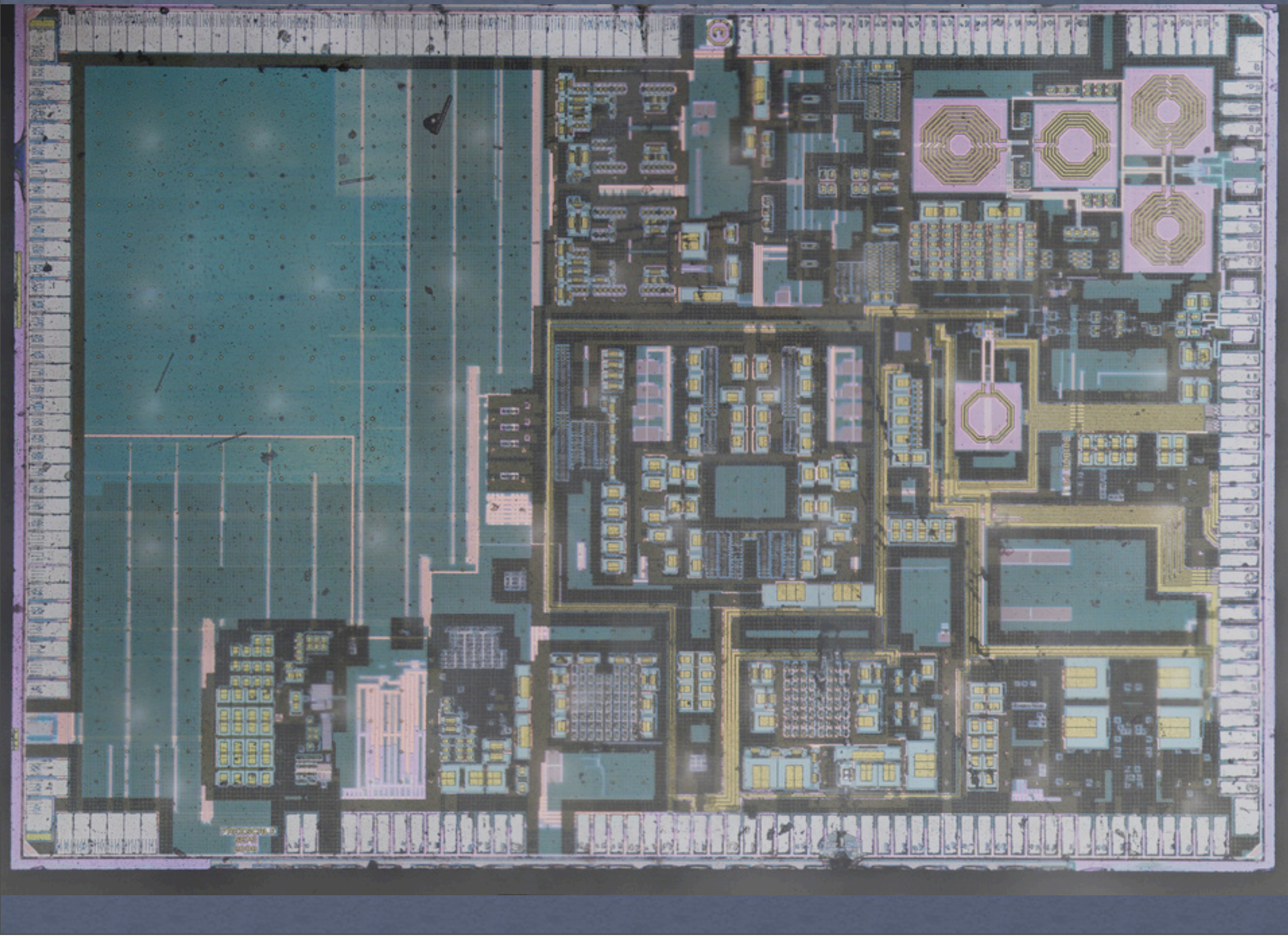
- Execution begins in Mask ROM at 0x0000:0000.
- ROM copies Flash into RAM at 0x0040:0000.
- ROM branches to 0x0040:0000.

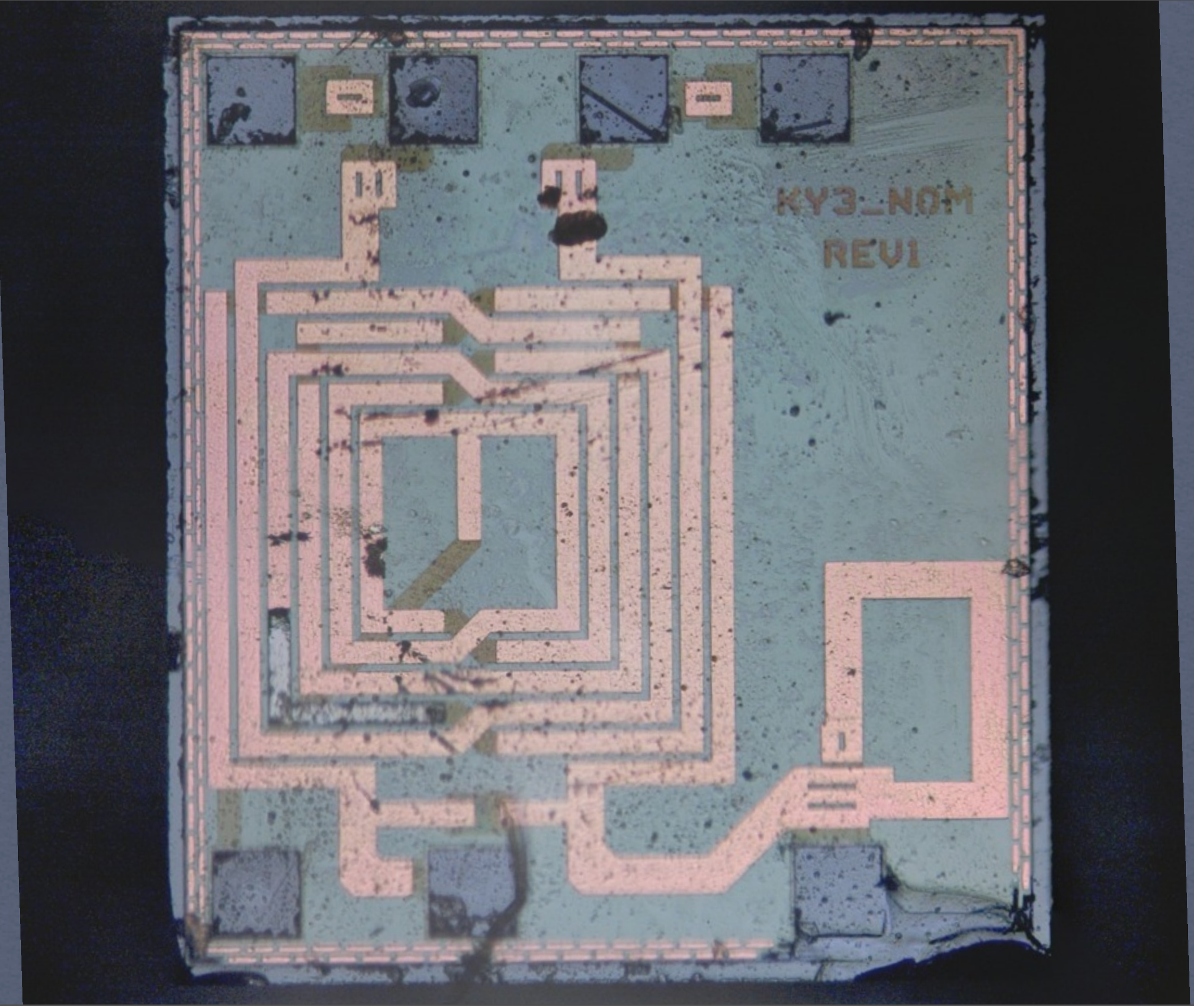
Accessing Flash

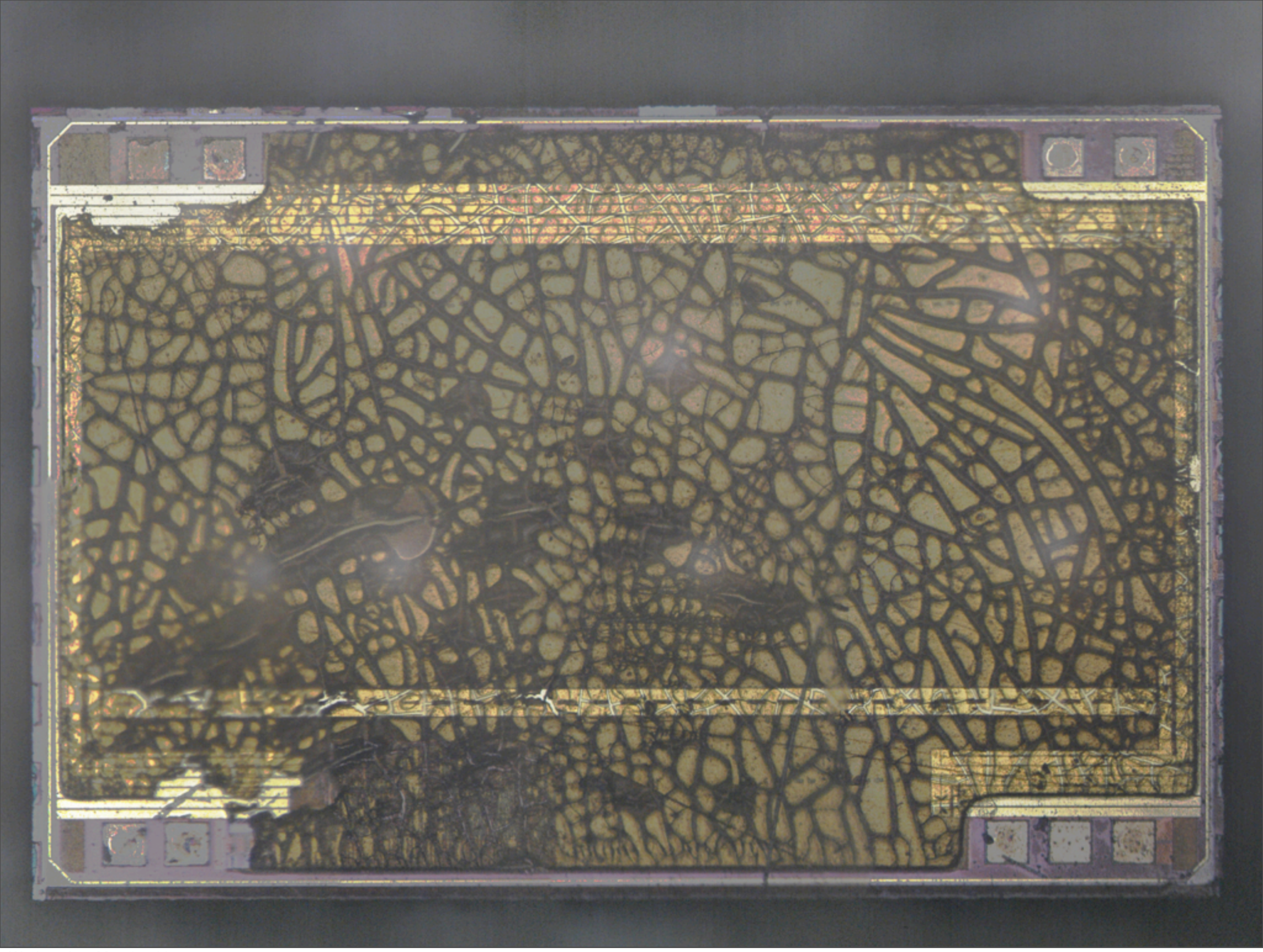
- The ARM7 can read and write Flash.
- It just isn’t mapped into memory.
- Instead, you use a serial port.



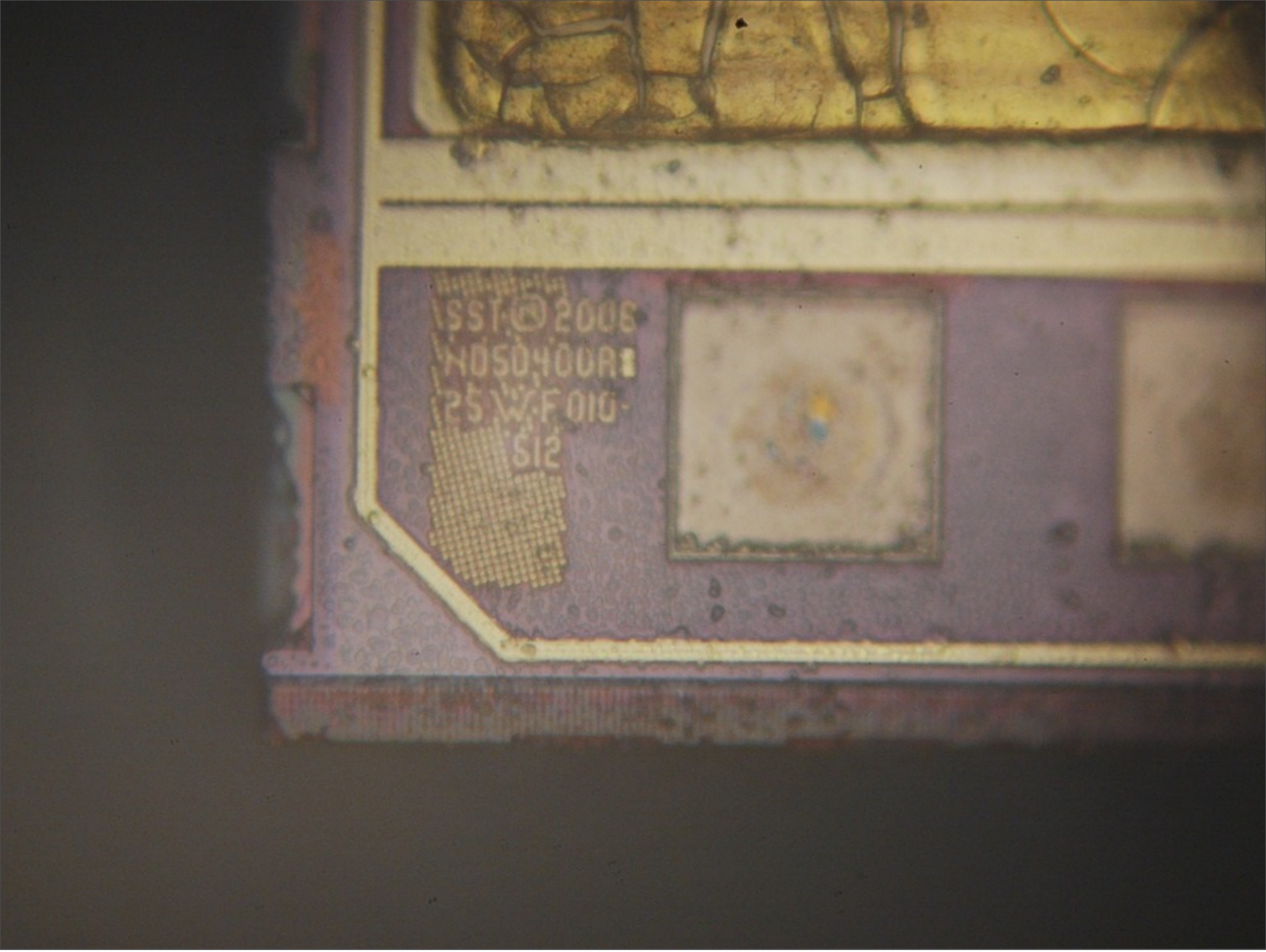
Wednesday, May 25, 2011




KY3_NOM
REV1

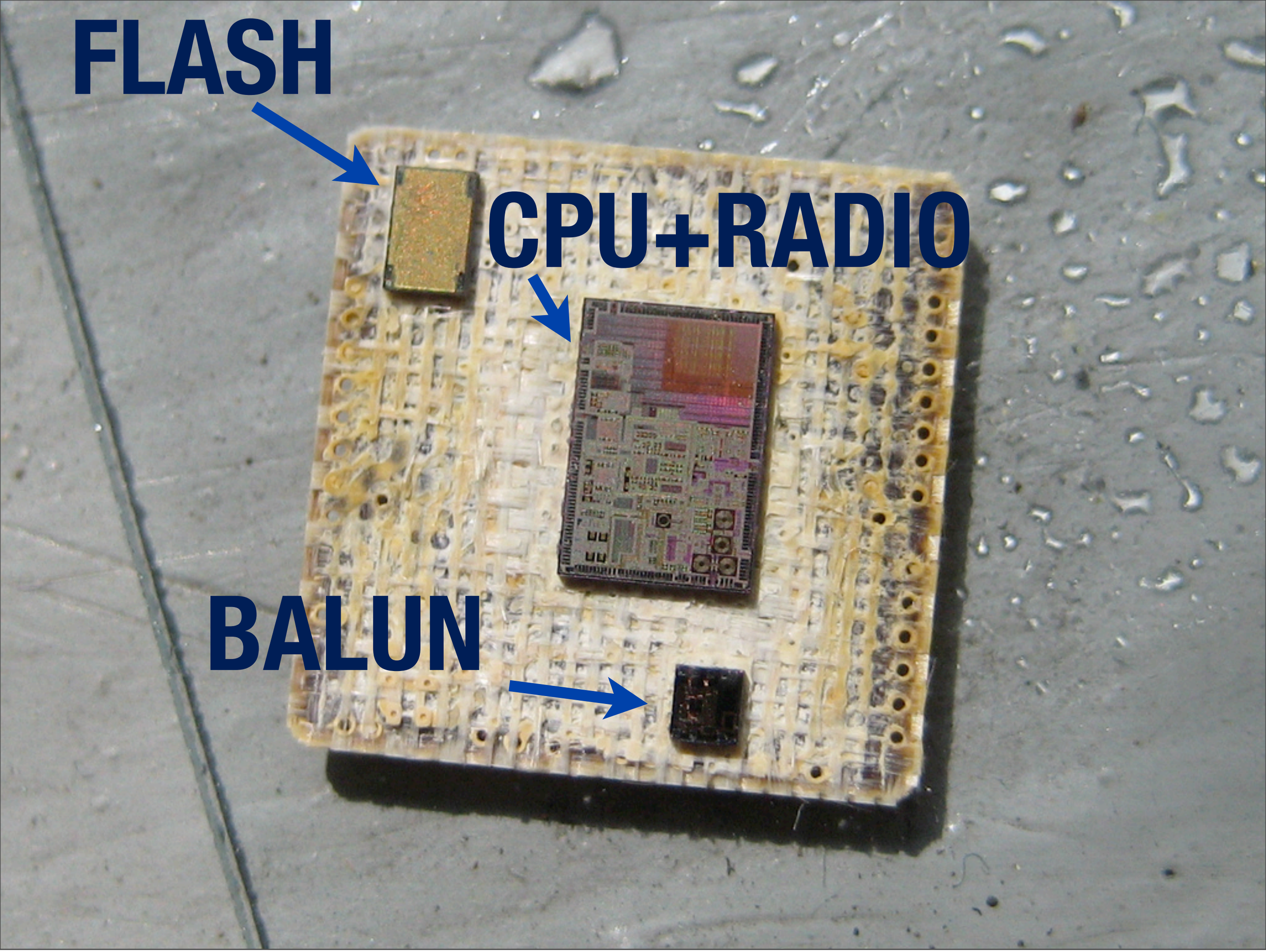


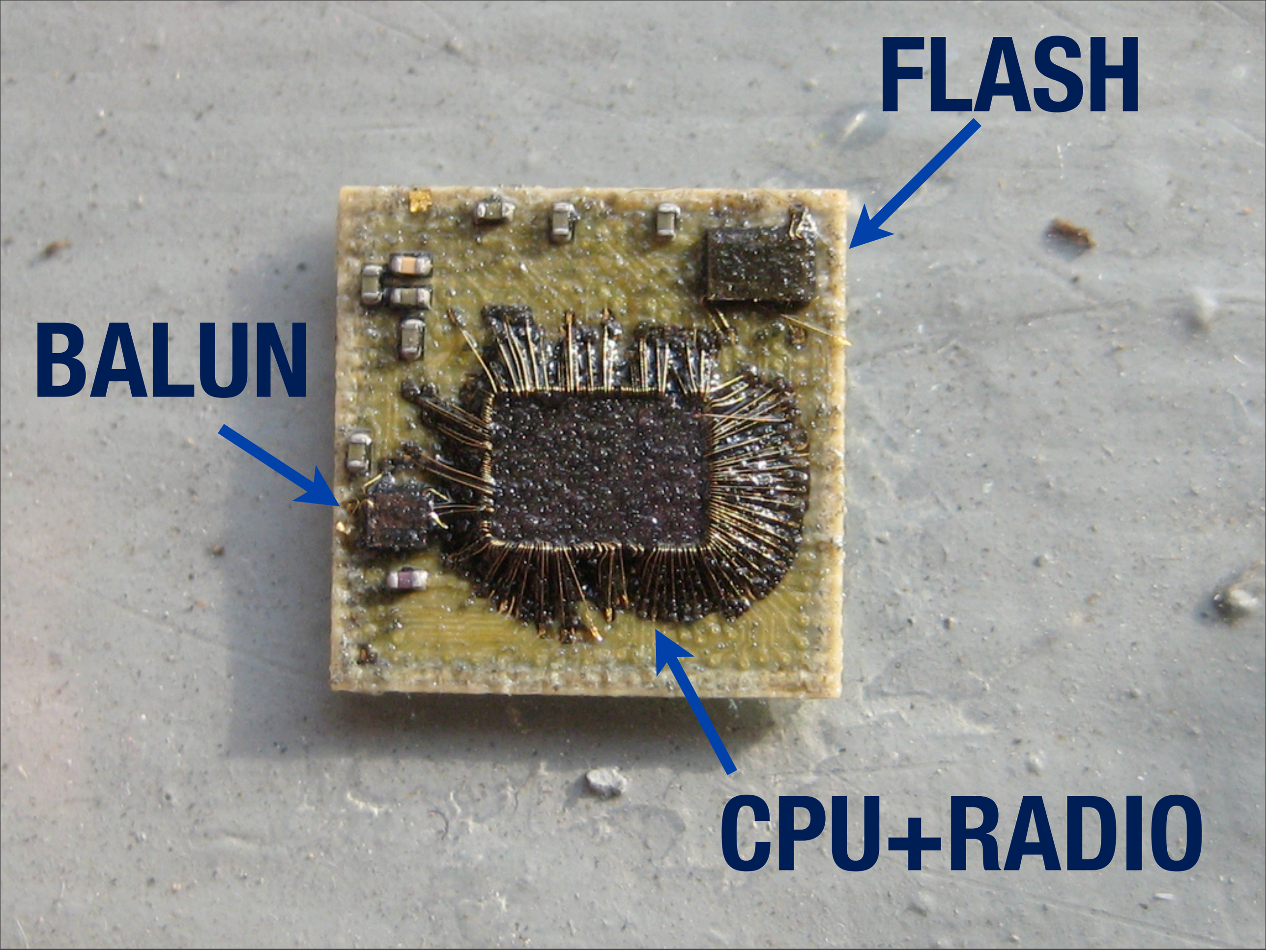
Wednesday, May 25, 2011



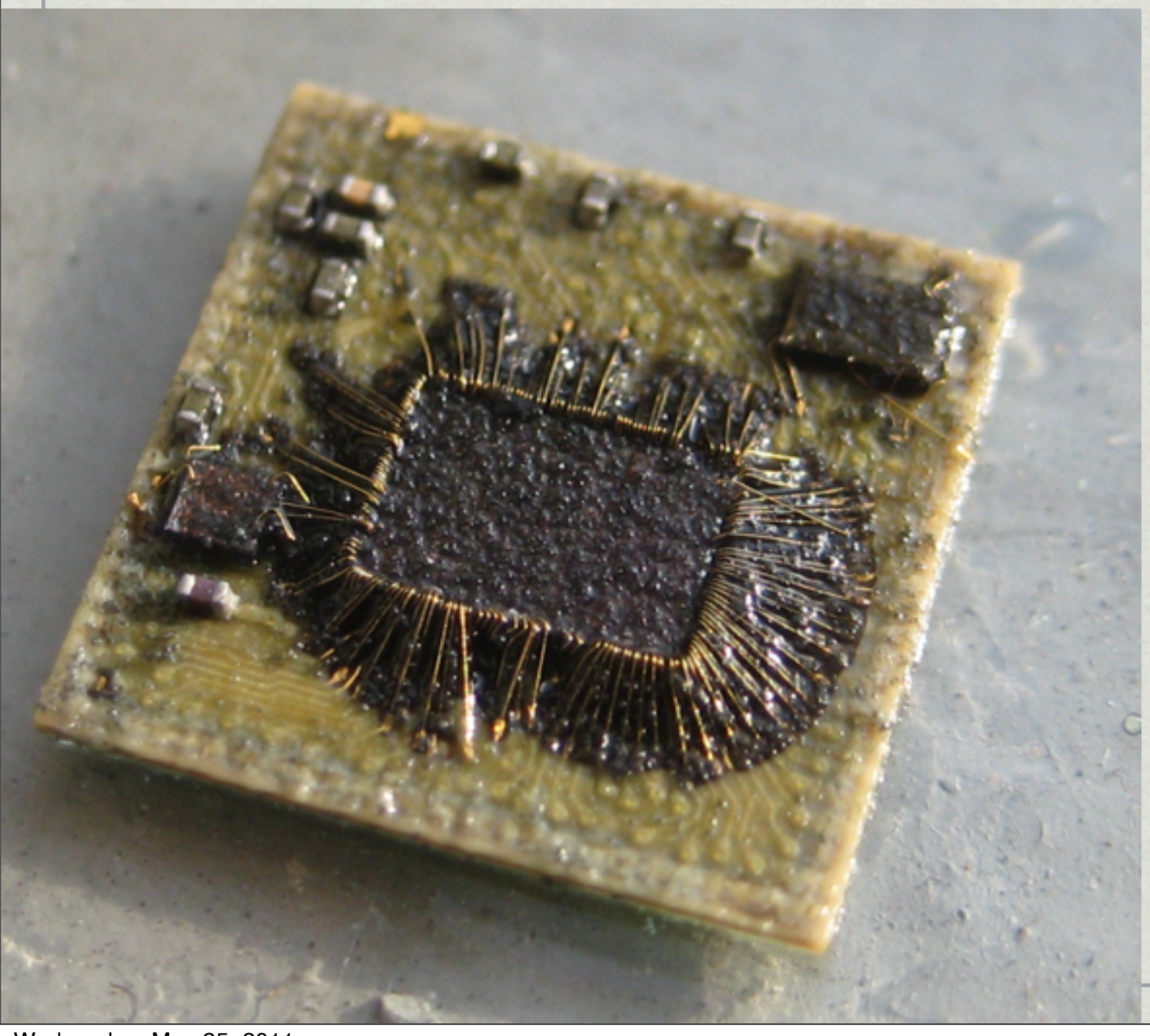
Wednesday, May 25, 2011


WSS(R)2006
WDSD400A
RSWF010-
S12


FLASH
CPU+RADIO
BALUN


FLASH
BALUN
CPU+RADIO

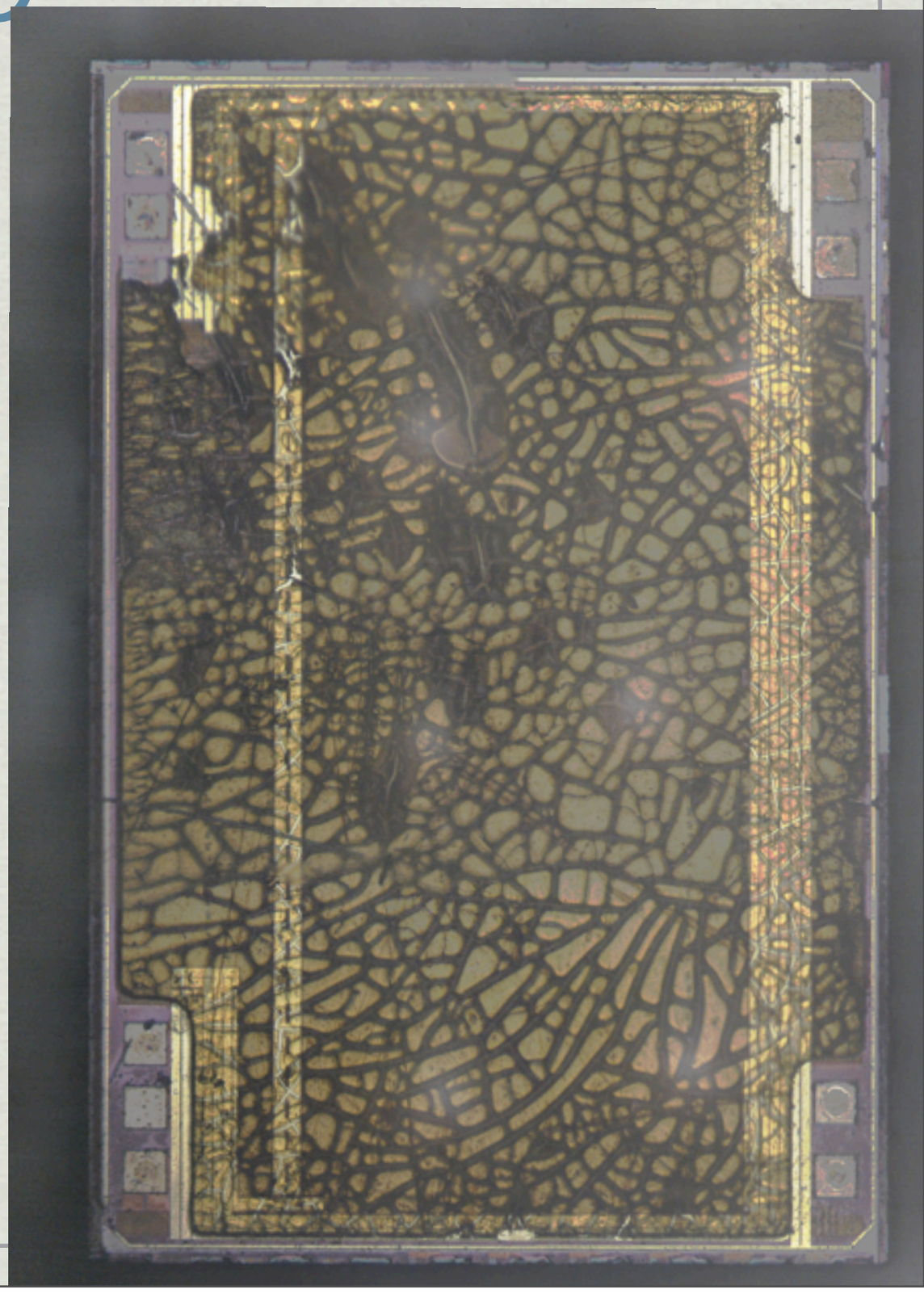
Three Chips



- ARM7+Radio
- Analog Balun
- SST25WF010 Flash

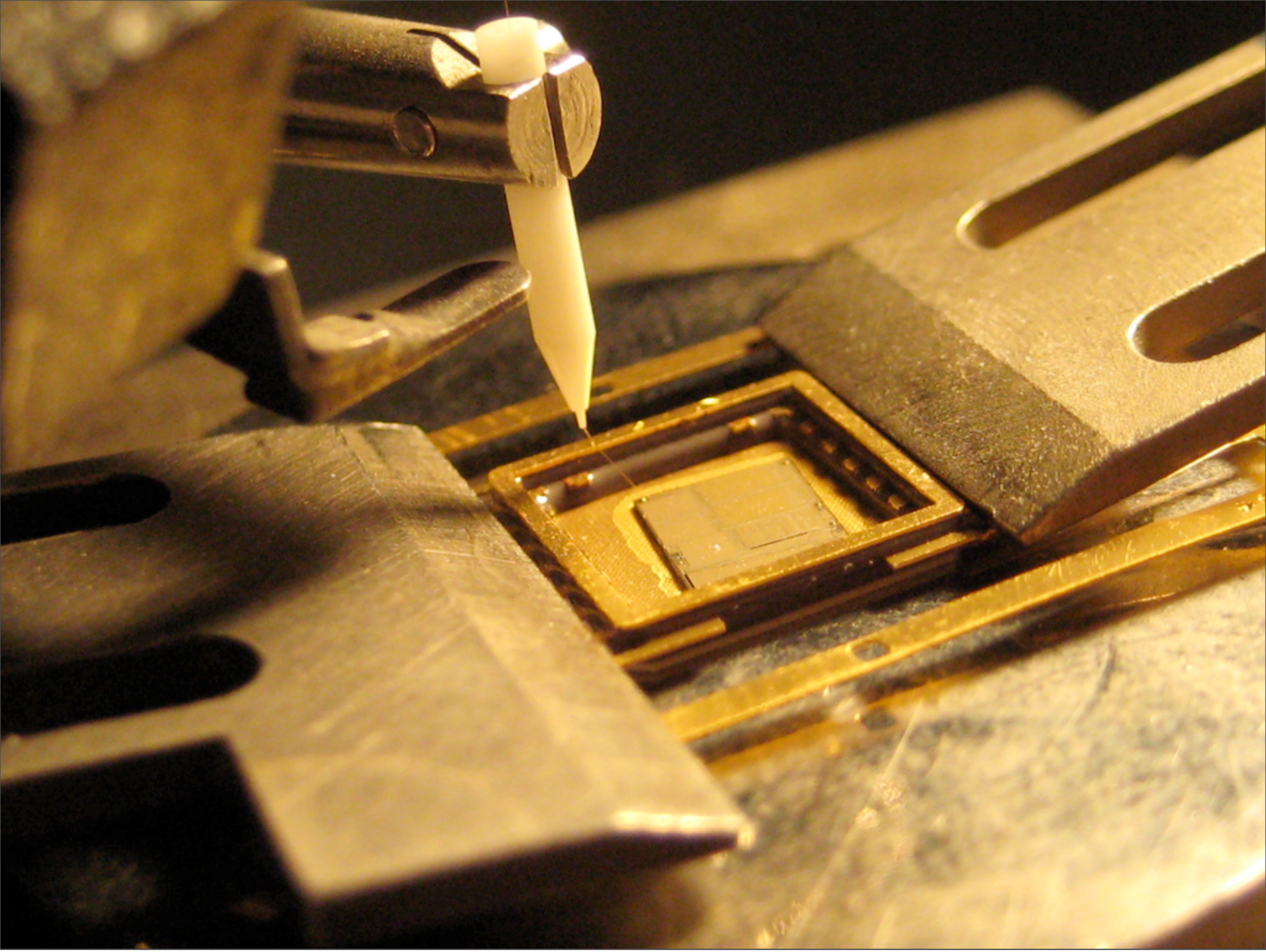
SST25WF010

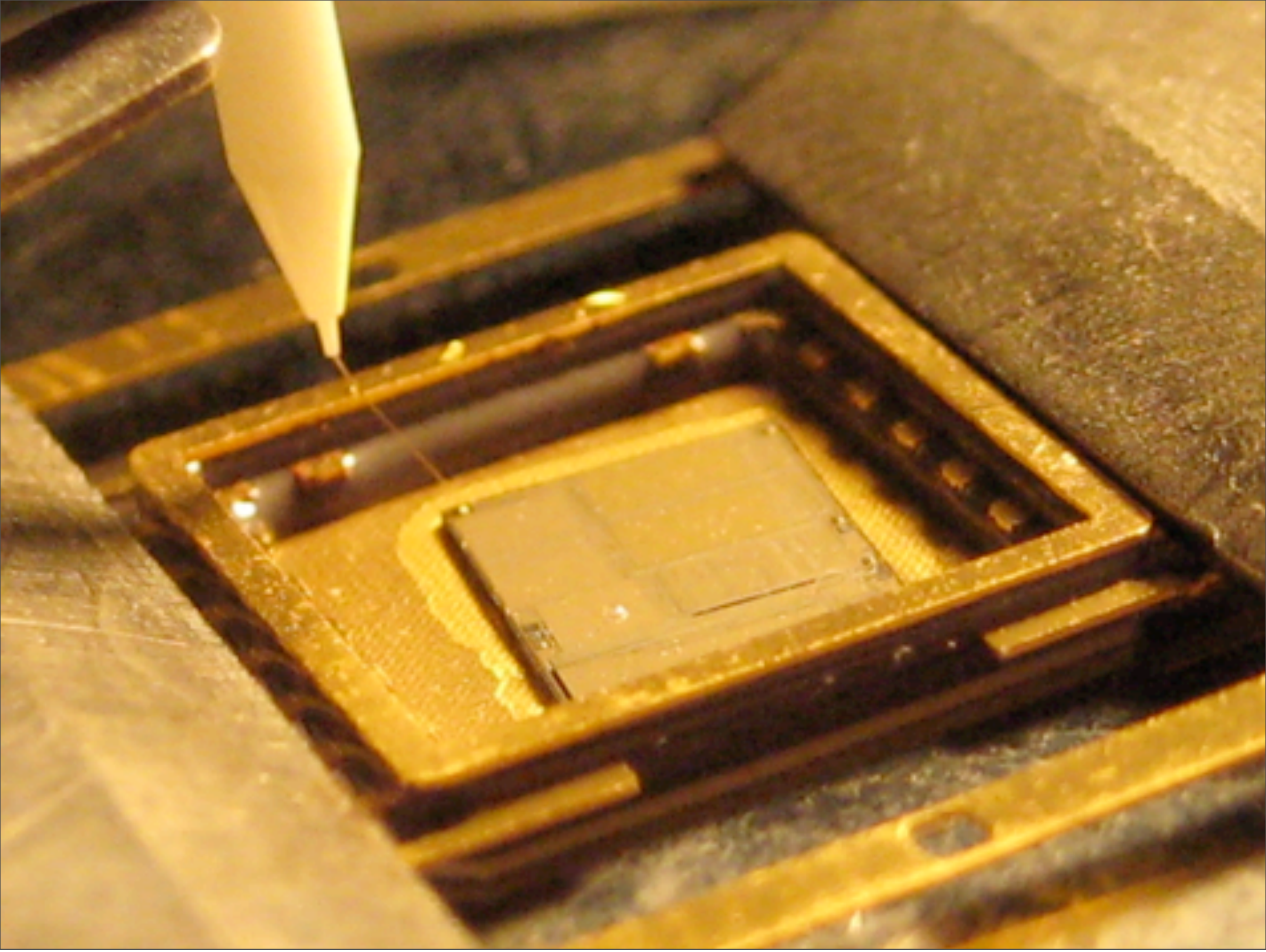
- Serial Peripheral Interface
- No protection!



Rebonding Attack

- Dissolve the packaging with acid.
- Break the bonding wires.
- Rebond just the SST25WF010 into a new package.
- Read it!



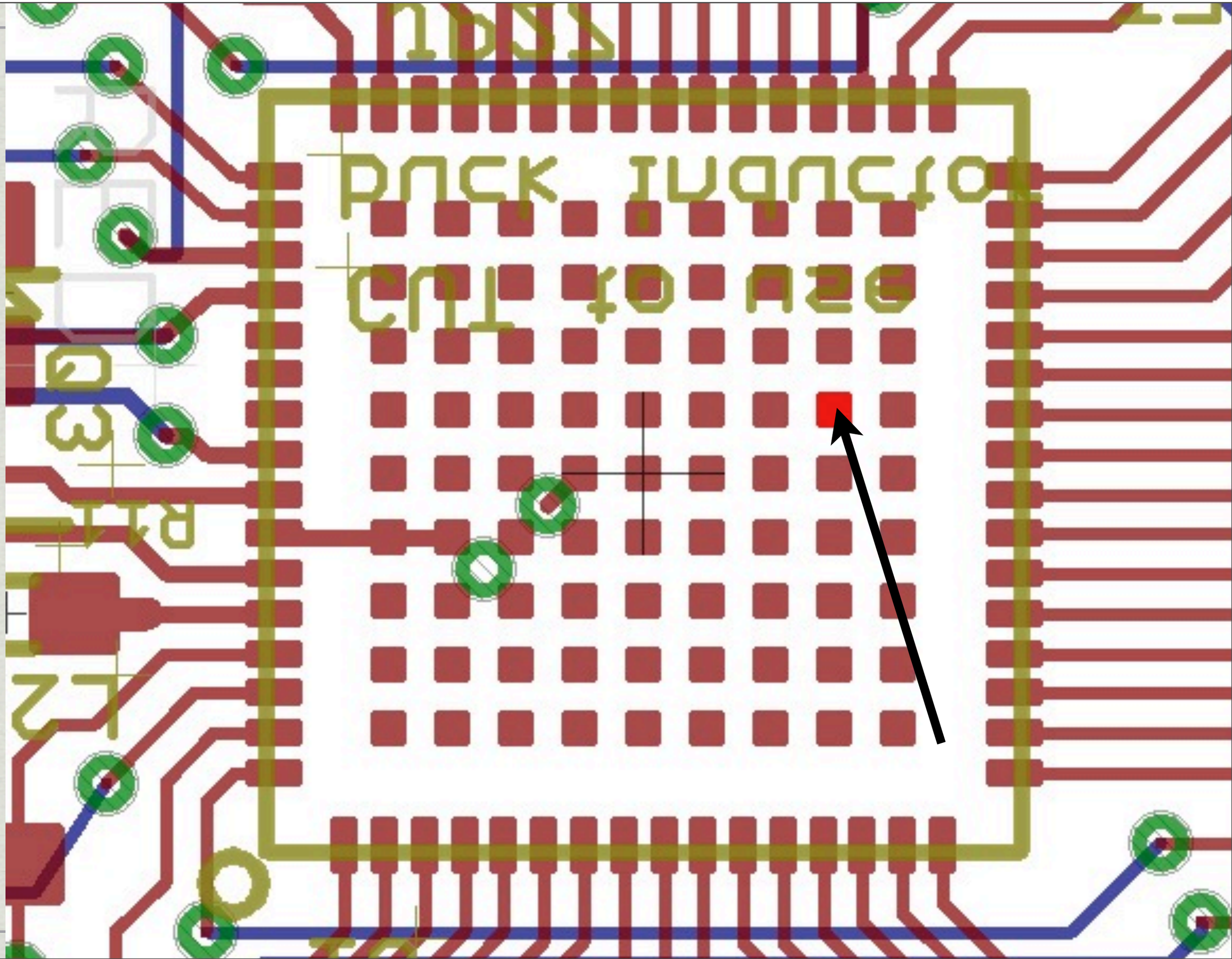


Rebonding Attack

- No trouble for funded attacker.
  - $5000 USD for a used wirebonder.
- Inconvenient, but affordable for a hobbyist.
  - Visit a Materials Science department.
  - Buy lots of pizza and beer.

Cheaper Attack

- Flash and CPU are on separate dies.
- CPU unlocks if Flash does *not* say `SECU'
- What if we damage Flash temporarily?



Cheaper Attack

- Pin 133 (VREG_NVM)
  - Voltage regulator for the Flash chip!
    - Externally accessible!
- Voltage Regulators
  - Defend against short-circuits!

Attack Hardware

- Redbee
  - MC13224 and FTDI
  - JTAG and Serial access.
- Modified Redbee
  - Pin 133 goes to a jumper.
  - Shorting the jumper disabled Flash.

Wednesday, May 25, 2011

Manufacturing a Board

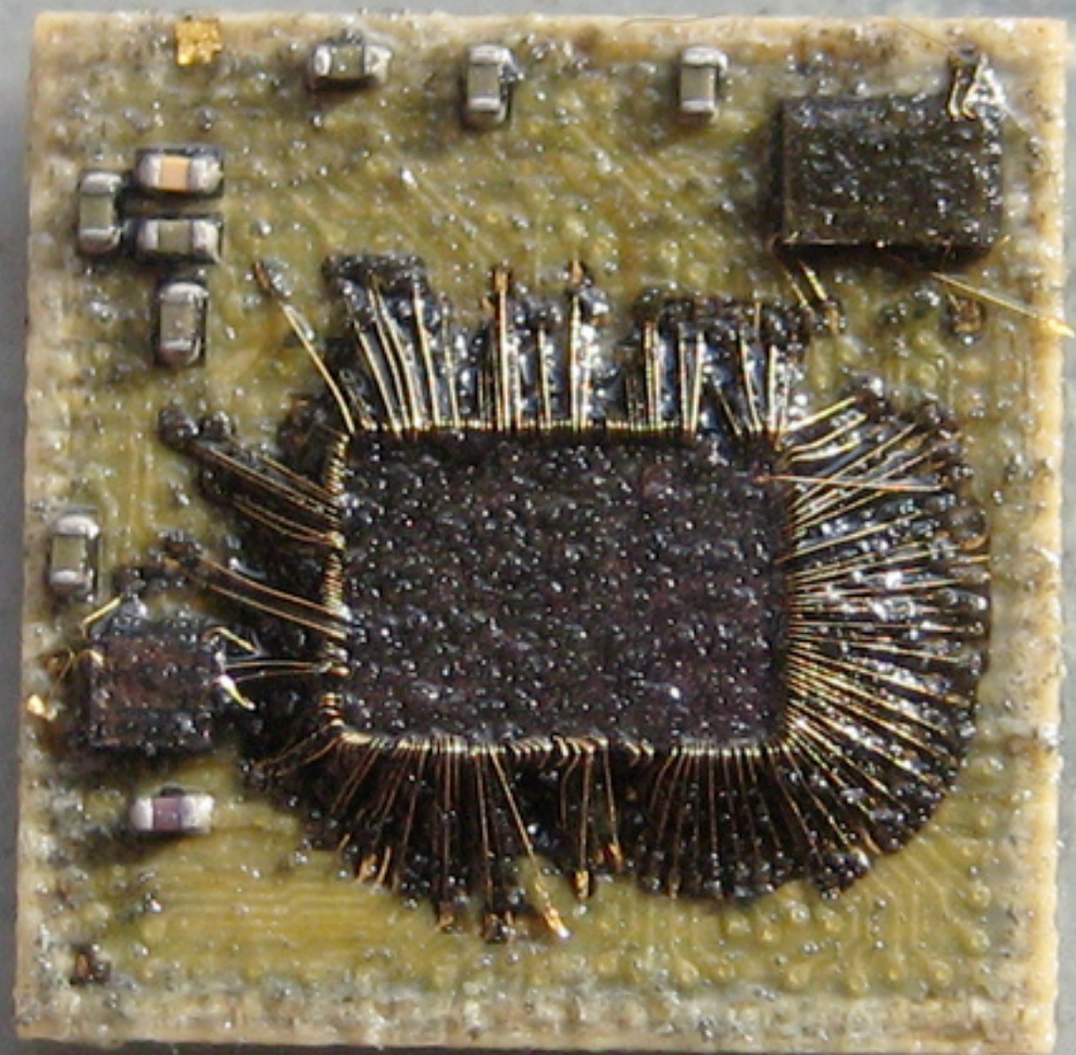
- CAD files go to a factory in China.
  - $100 for a panel.
    - $10 and a delay for a single board.
- Modifying an open design is easy.
  - Just like patching software.

Attack Technique

- Move the MC13224 to the attack board.
- Short Pin 133 to GND with the new jumper.
- Power up the device and connect to JTAG.
- Disconnect the short, restoring Flash.
- Use JTAG to read Flash into your workstation.

Firmware Patch

- The first four bytes of the image will be “SECU”.
- Change them to “OKOK” and reflash.
- The chip is now unlocked!
- Hook a debugger and fuzz away!



Wednesday, May 25, 2011

Conclusions

- The Freescale MC13224 is easily extractable.
  - $10 USD in components.
  - $100 USD in soldering equipment.
- Other system-on-package devices?

Additional Info

- Article at http://travisgoodspeed.com
- Other articles worth reading:
  - Reverse engineering embedded radio firmware.
  - Sniffing a Microsoft 2.4GHz Keyboard.