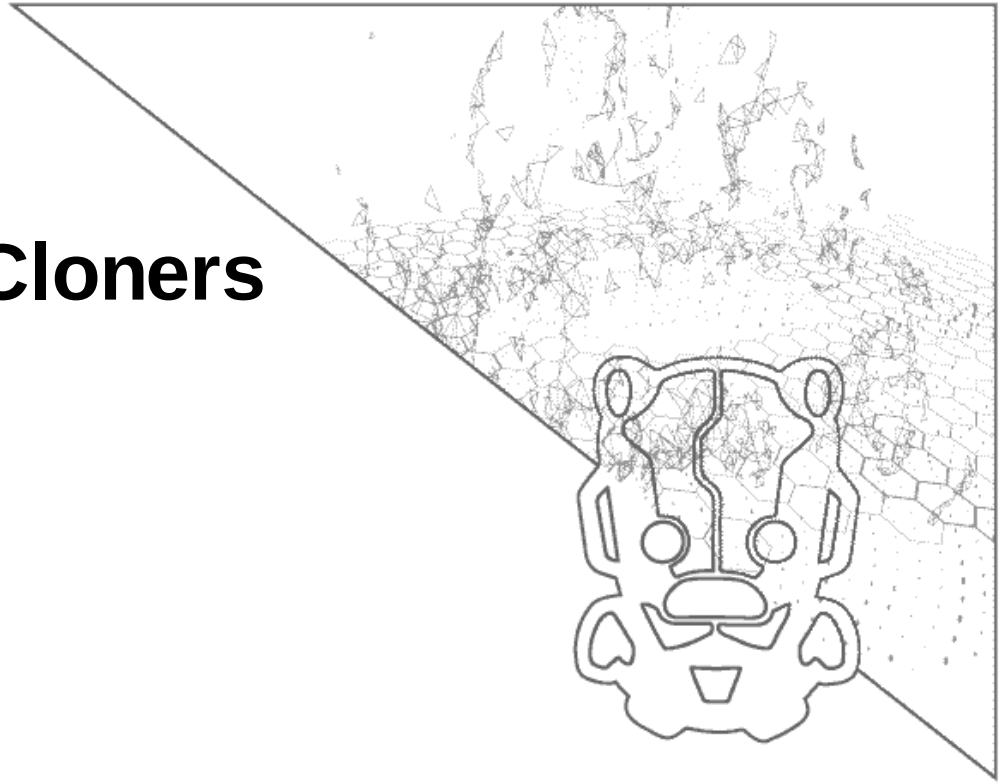
Secure Elements vs Cloners

A Case Study

Andrew D. Zonenberg, Ph.D.
Principal Security Consultant



IOActive®

IOActive Presentation Content

Legal Notices

- **Disclaimer Notification**
  The views, opinions, findings, conclusions, positions, and/or recommendations expressed herein are those of the authors individually and do not necessarily reflect the views, opinions, or positions of IOActive, Inc.
- **No Warranties or Representations**
  The information presented herein is provided "AS IS" and IOActive disclaims all warranties whatsoever, whether express or implied. Further, IOActive does not endorse, guarantee, or approve, and assumes no responsibility for nor makes any representations regarding the content, accuracy, reliability, timeliness, or completeness of the information presented. Users of the information contained herein assume all liability from such use.
- **Publicly Available Material**
  All non-IOActive source material referenced in this presentation was obtained from the Internet without restriction on use.
- **Fair Use**
  This primary purpose of this presentation is to educate and inform. It may contain copyrighted material, the use of which has not always been specifically authorized by the copyright owner. We are making such material available in our efforts to advance understanding of cyber safety and security. This material is distributed without profit for the purposes of criticism, comment, news reporting, teaching, scholarship, education, and research, and constitutes fair use as provided for in section 107 of the Copyright Act of 1976.
- **Trademarks**
  IOActive, the IOActive logo and the hackBOT logo are trademarks and/or registered trademarks of IOActive, Inc. in the United States and other countries. All other trademarks, product names, logos, and brands are the property of their respective owners and are used for identification purposes only.
- **No Endorsement or Commercial Relationship**
  The use or mention of a company, product or brand herein does not imply any endorsement by IOActive of that company, product, or brand, nor does it imply any endorsement by such company, product manufacturer, or brand owner of IOActive. Further, the use or mention of a company, product, or brand herein does not imply that any commercial relationship has existed, currently exists, or will exist between IOActive and such company, product manufacturer, or brand owner.
- **Copyright**

Researcher and Briefer

Andrew D. Zonenberg, Ph.D.

Principal Security Consultant

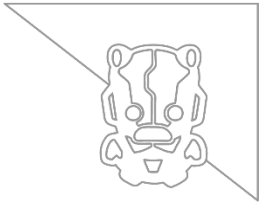
Bio: Andrew specializes in security at the hardware-software interface. His research interests range from probing of multi-gigabit serial interfaces to gate-level IC reverse engineering. In 2014, he taught the world's first university course on semiconductor reverse engineering.

He has presented at a wide range of industry and academic conferences, workshops, and events across North America and Europe.

andrew.zonenberg@ioactive.com
@azonenberg@ioc.exchange

IOActive.

The Big Picture



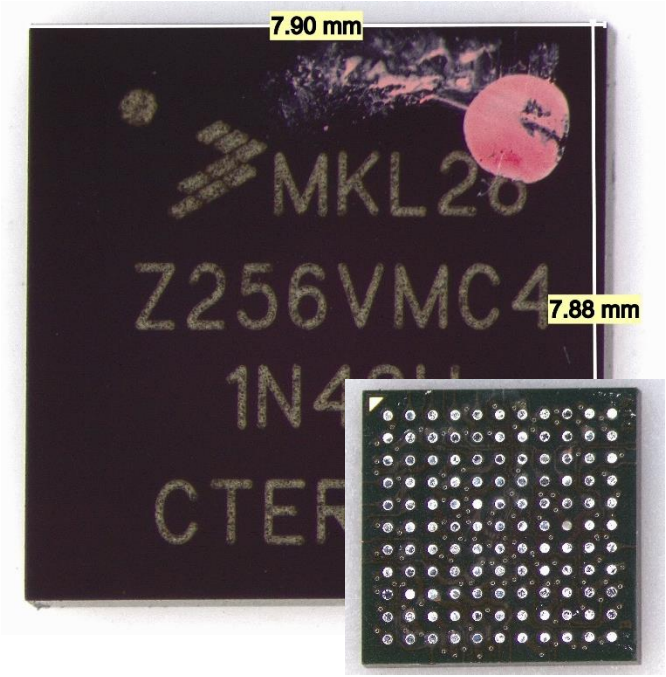
- Device manufacturers often use cryptographic mechanisms to vendor-lock accessories
- Third parties want to break these mechanisms to sell compatible accessories
- Let's see how this played out in one specific situation…

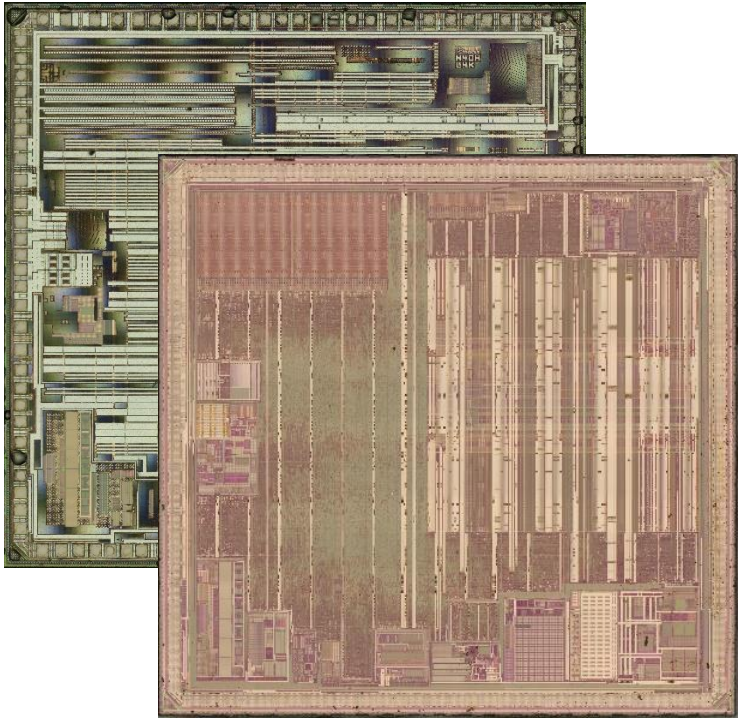
Case Study Overview

- Widely deployed (tens of millions sold) [redacted]
  - Multiple hardware generations
  - Two in particular are interesting to us
- Third party [redacted] exist on the market
  - Released shortly after major OEM hardware redesign
  - I wonder why?
- Let's dig deeper!

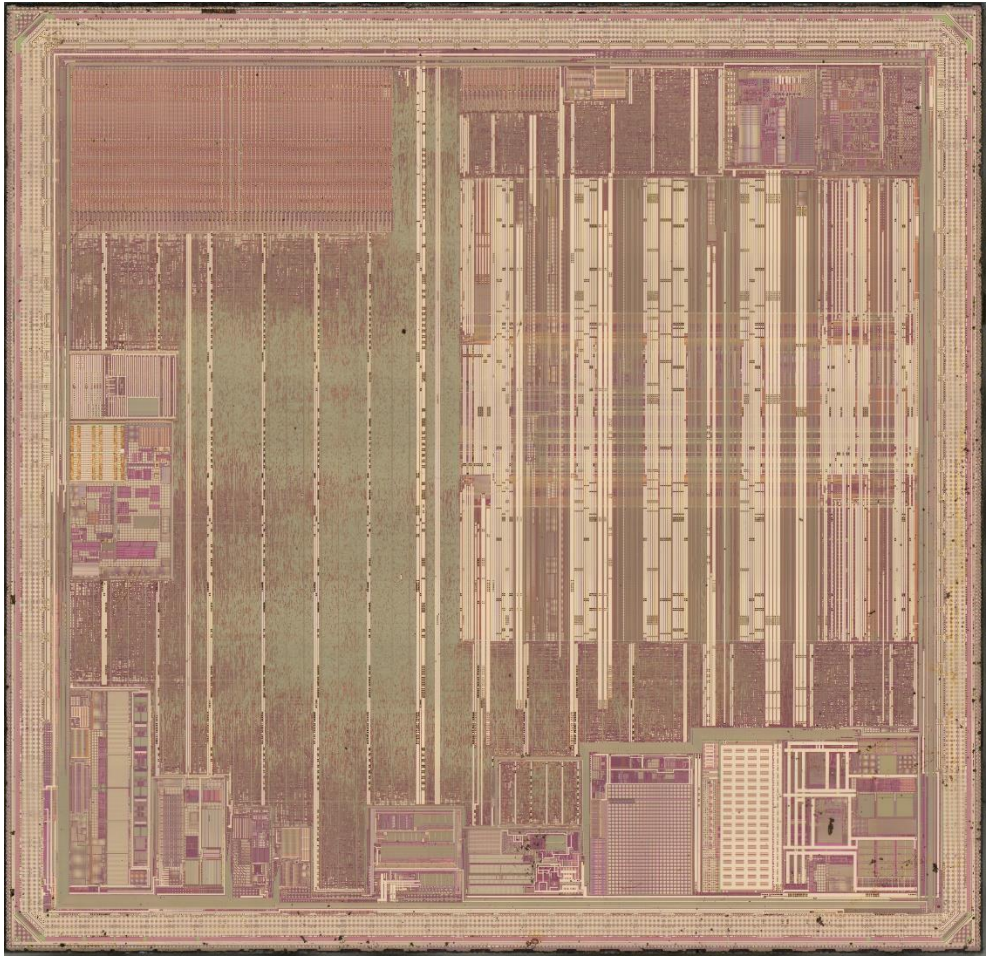
Old gen OEM product

- Freescale KL28 MCU





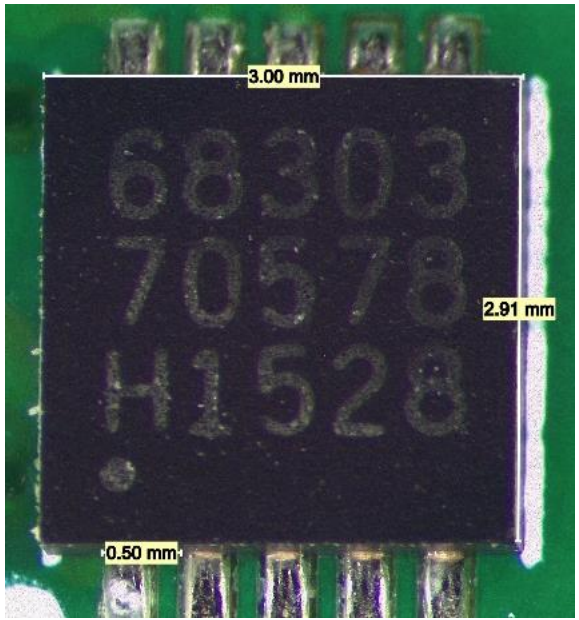
IOActive.

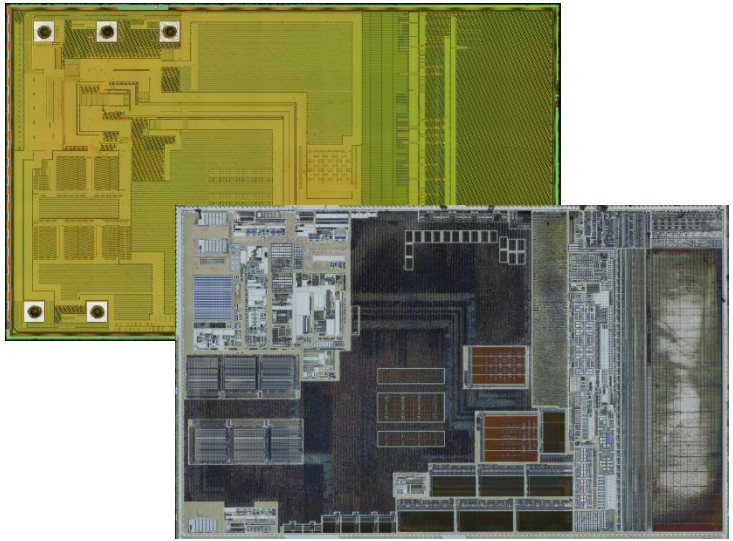


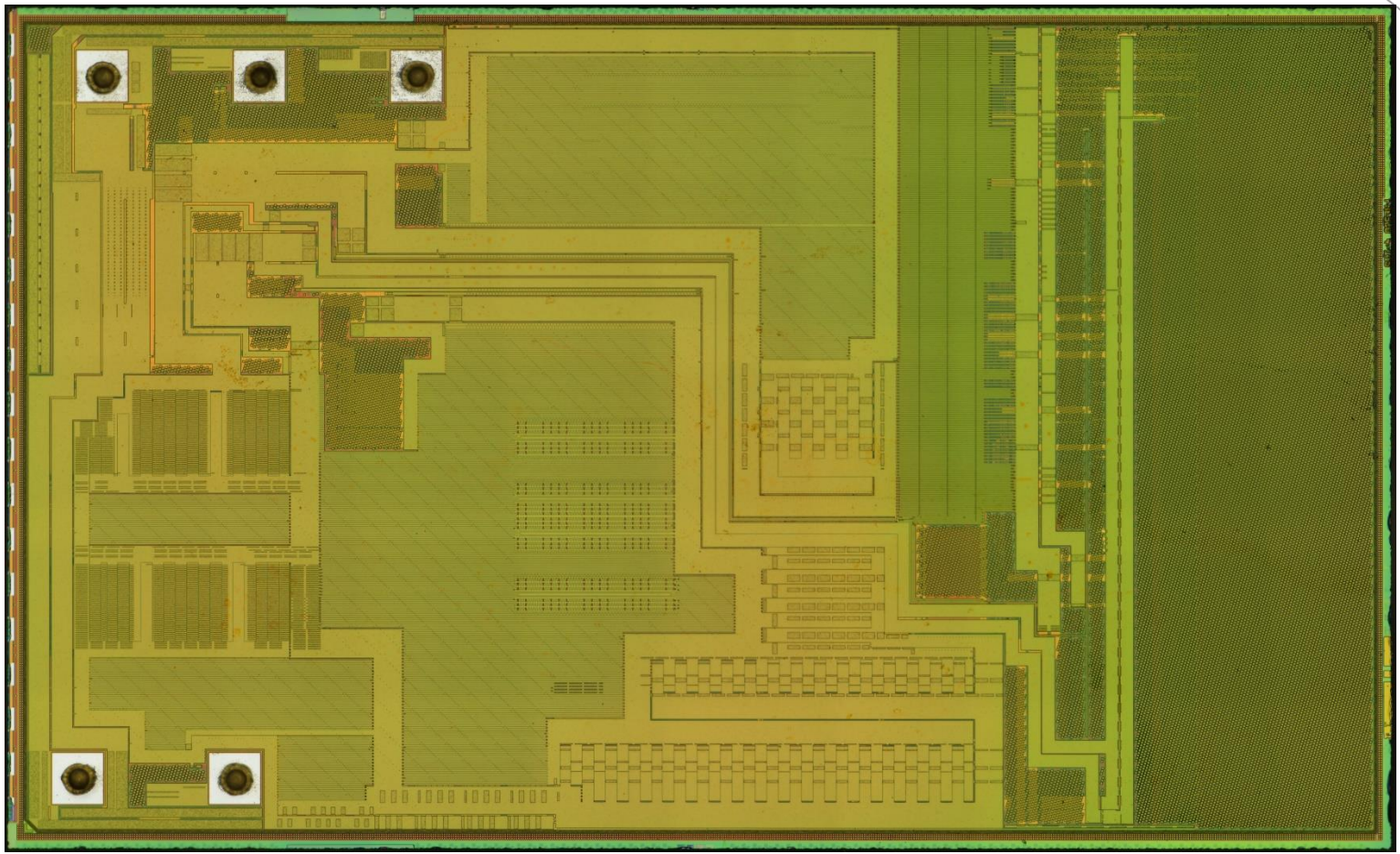
- Not super interesting
- Keys are elsewhere

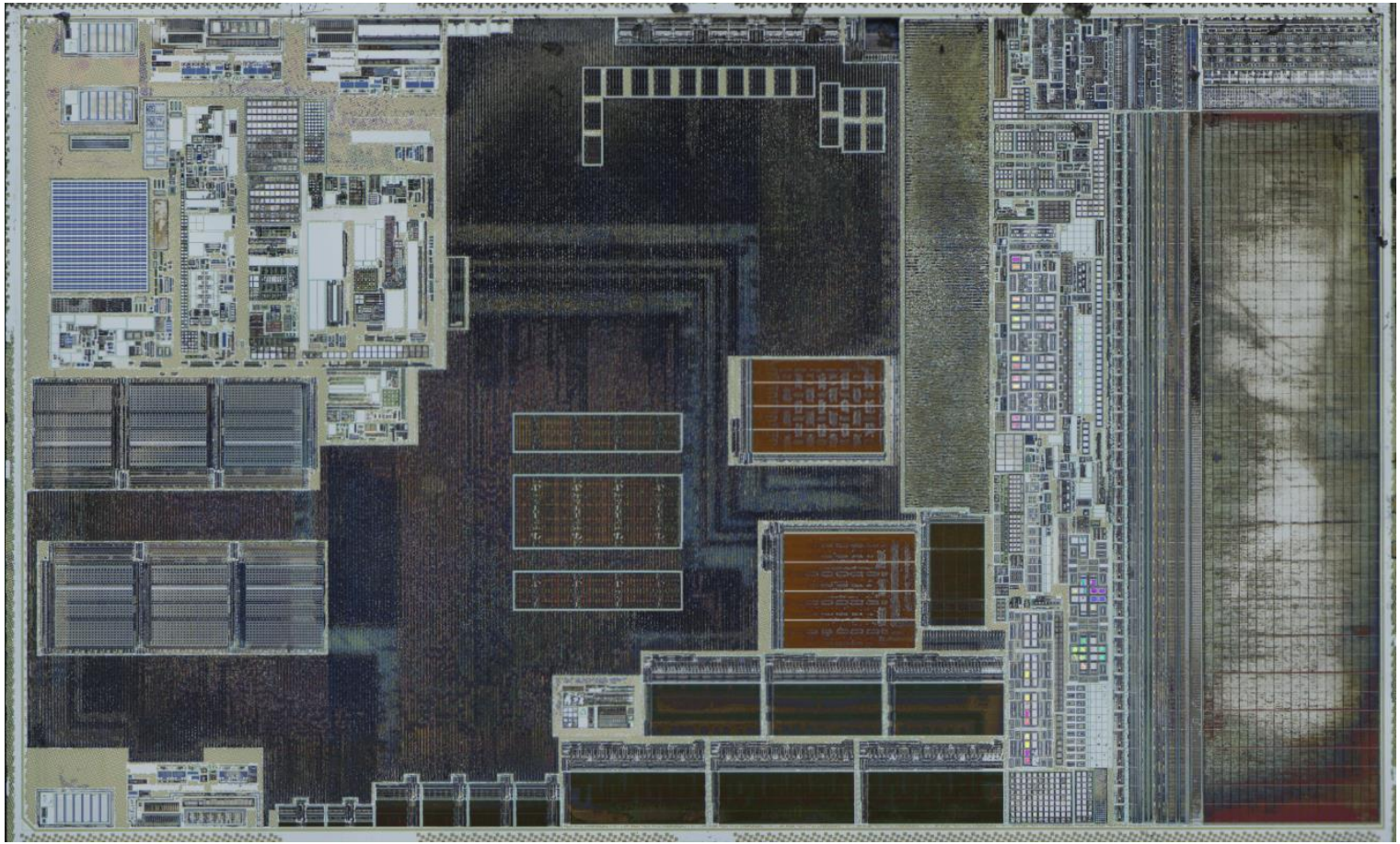
Old gen OEM product

- Infineon secure element



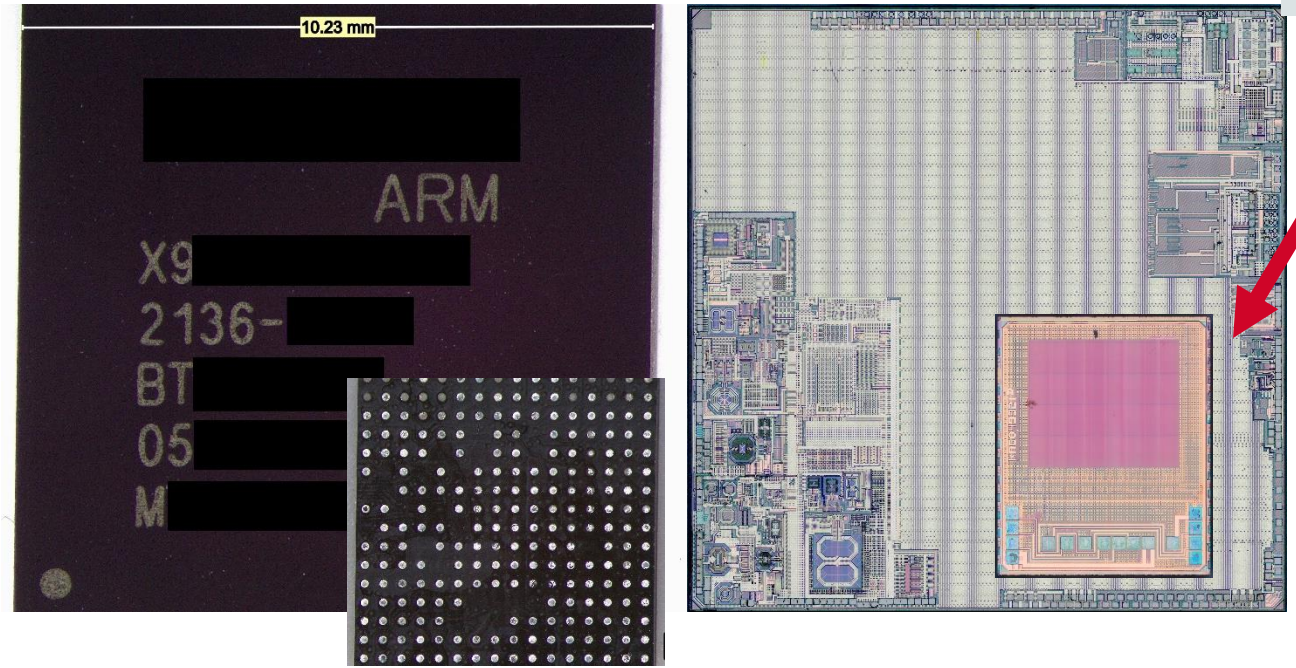




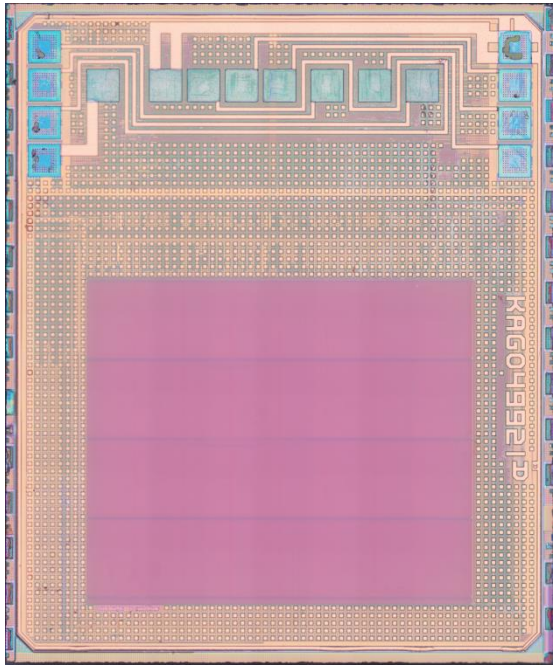


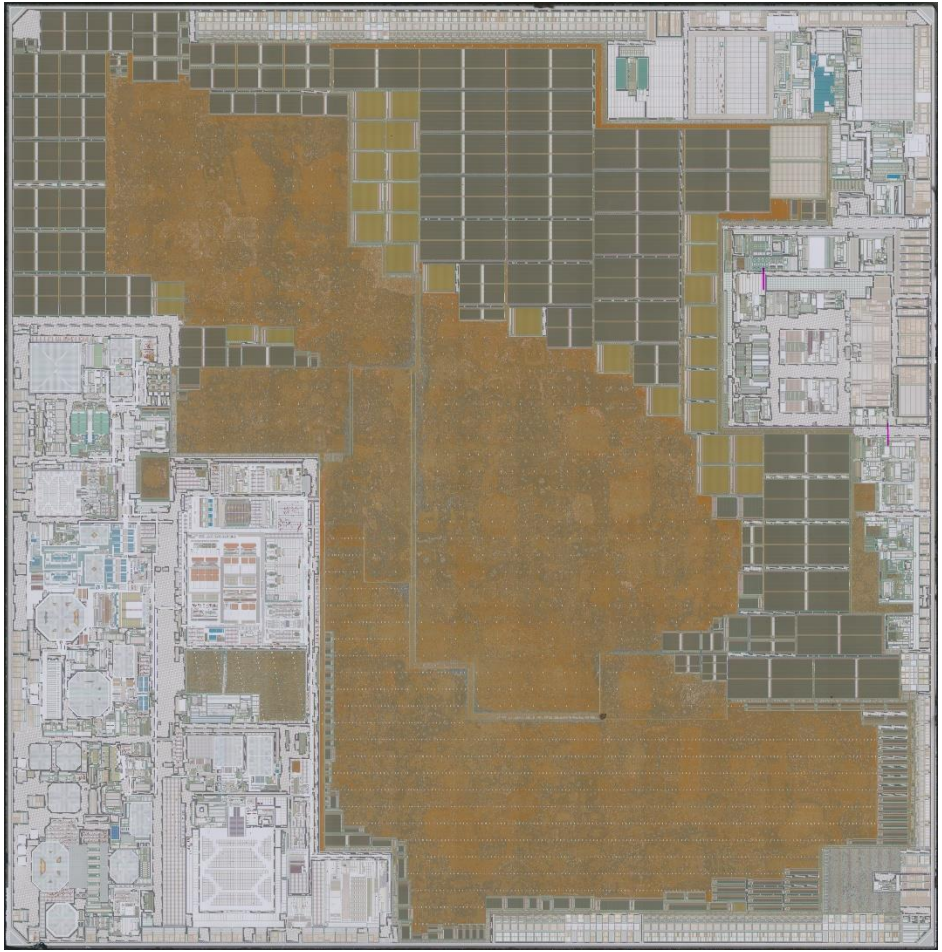
New gen OEM product

- All in one SoC with OEM branding



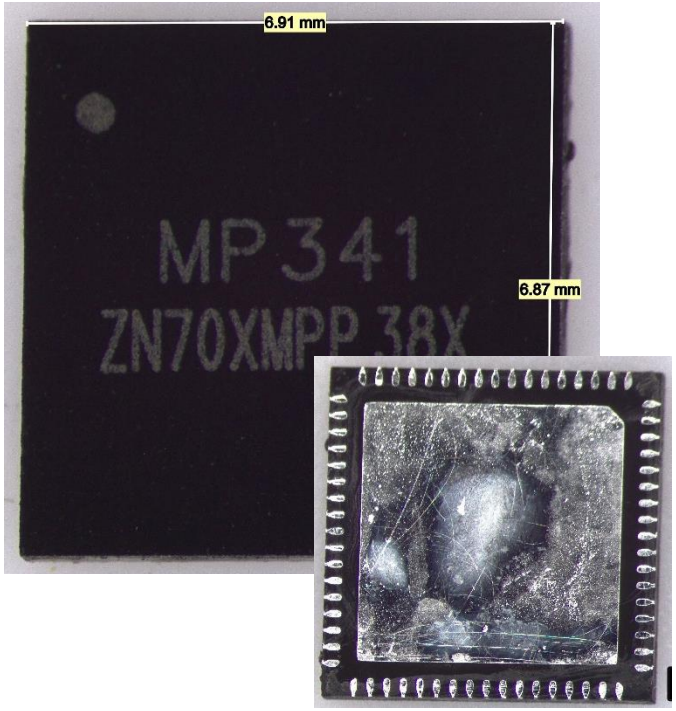
IOActive.



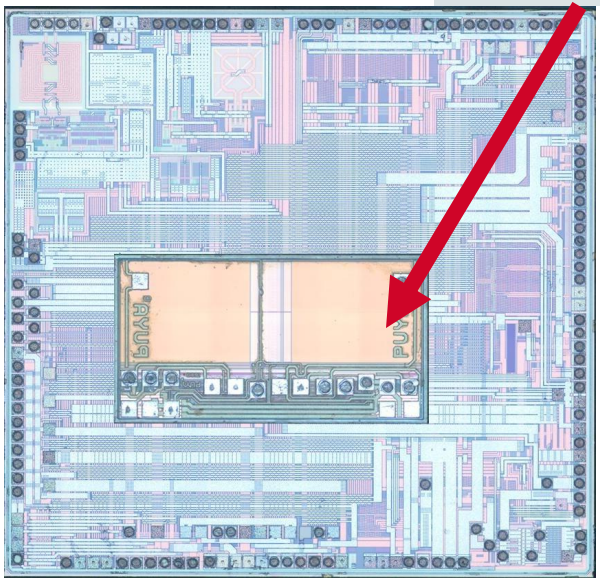


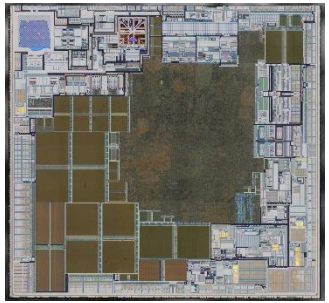
Third party

- Unidentified 55nm MCU

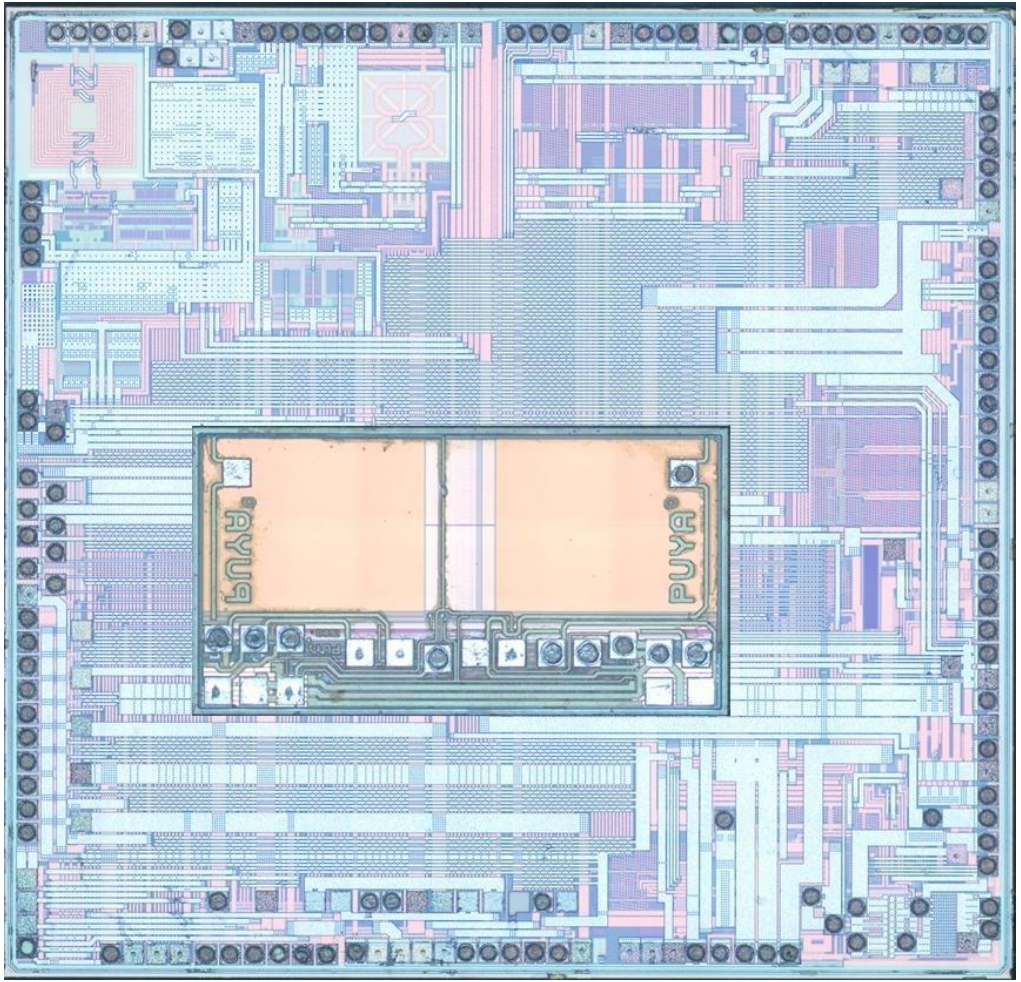


Stacked die
SPI flash

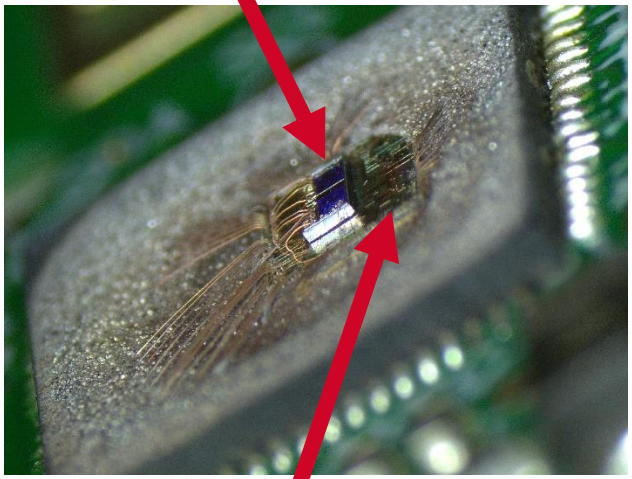




IOActive.

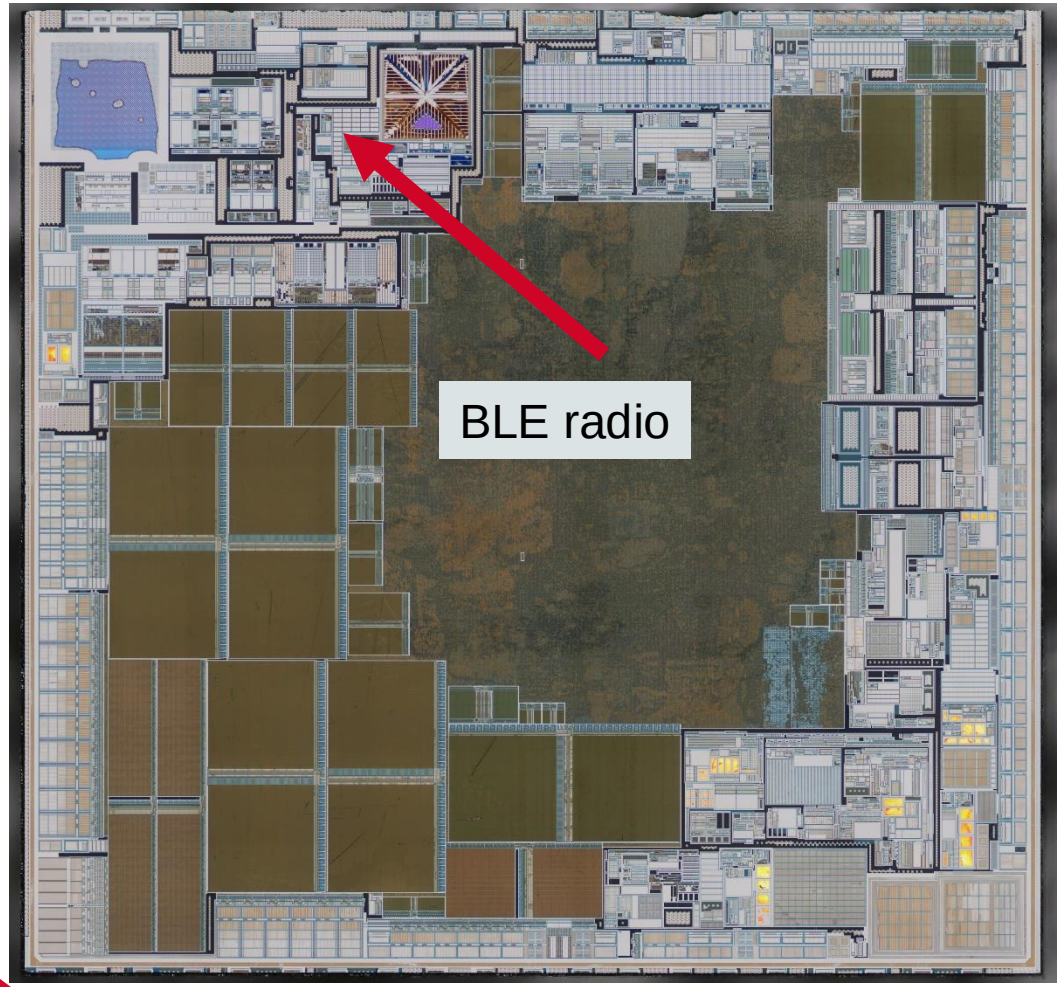


Flash die



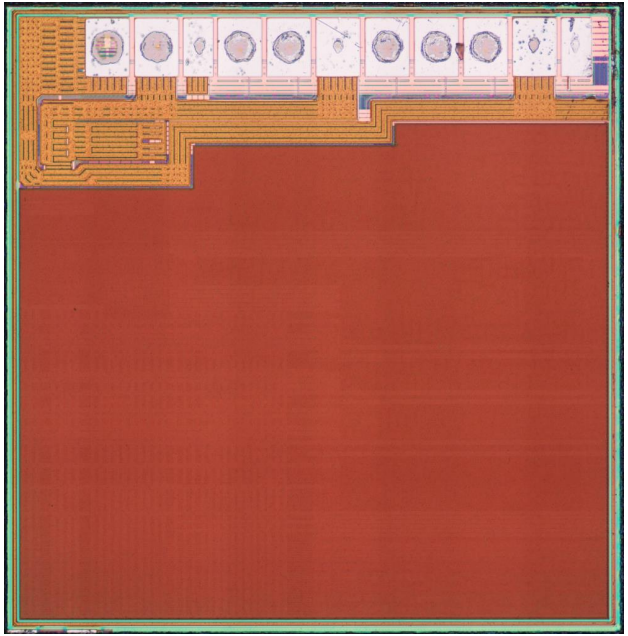
Logic die

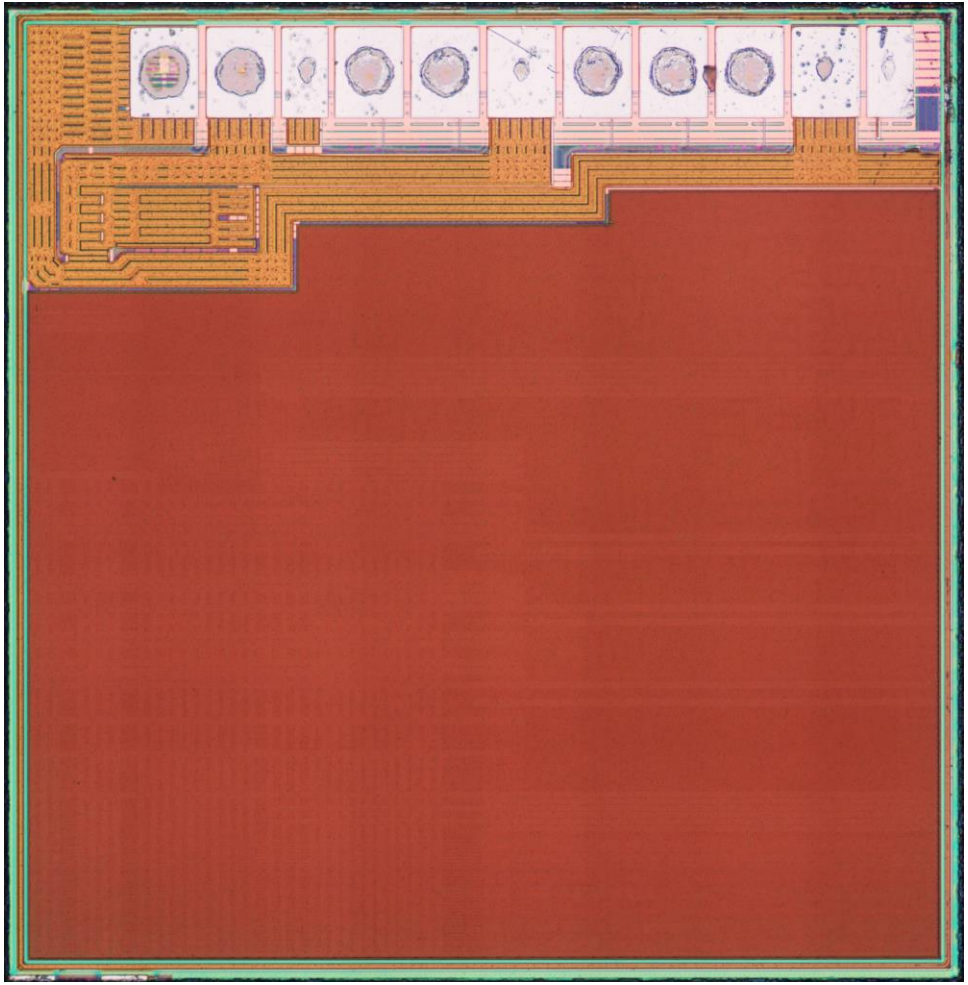
IOActive.

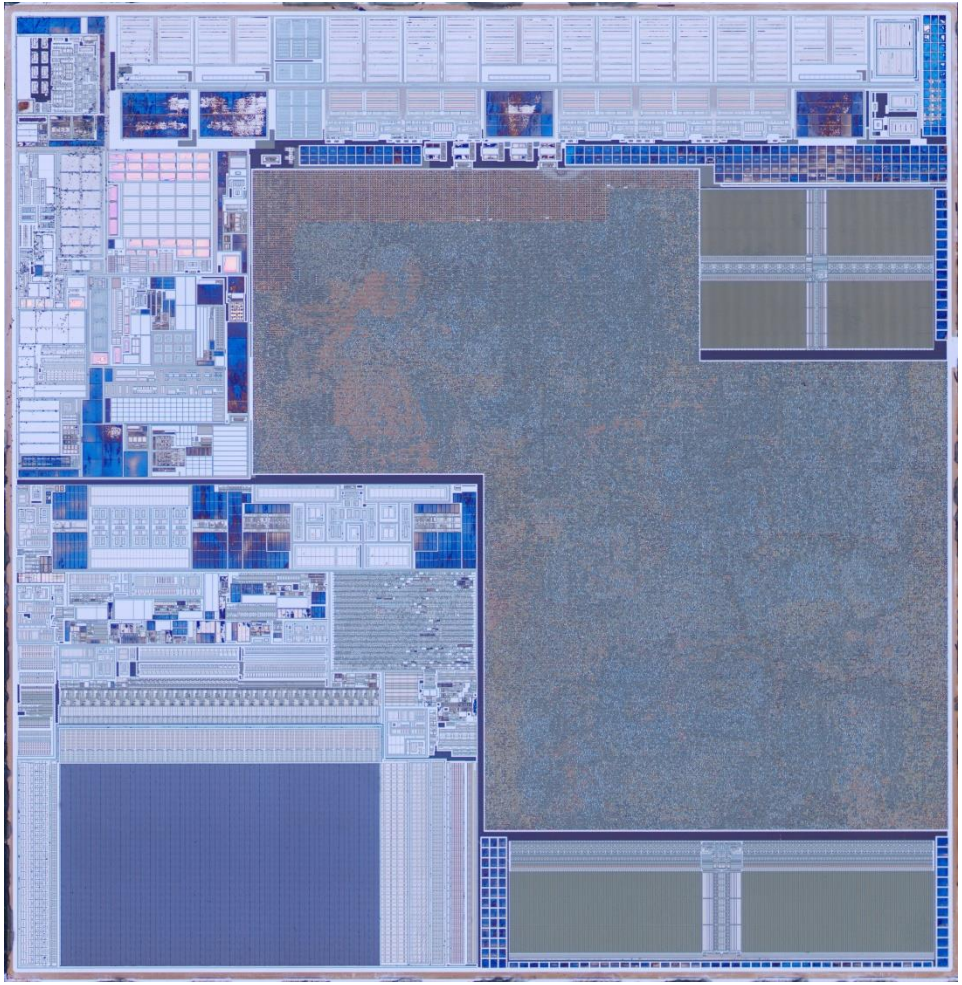


Third party

- Unidentified 55nm secure element



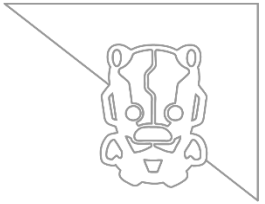




But why a secure element on the clone?

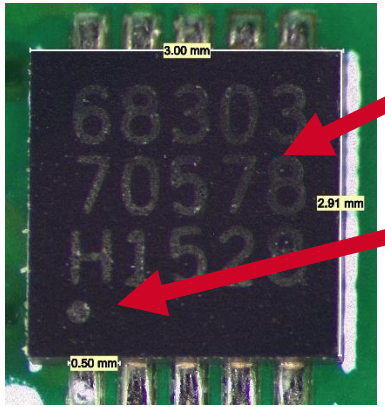
- Didn’t make a whole lot of sense to us at first
  - Just put the key in flash on your MCU
  - Crypto libraries etc work fine on a regular MCU

But why a secure element on the clone?



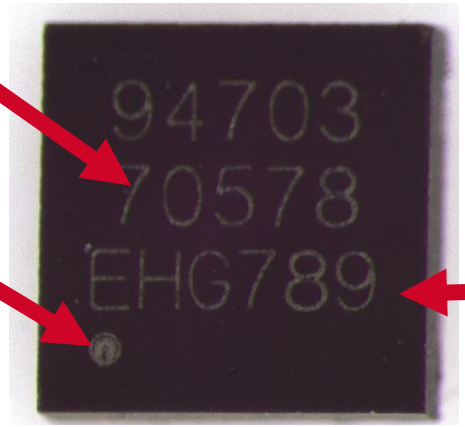
- Didn’t make a whole lot of sense to us at first
  - Just put the key in flash on your MCU
  - Crypto libraries etc work fine on a regular MCU
- Unless… you want the clone market to yourself!

Secure Elements

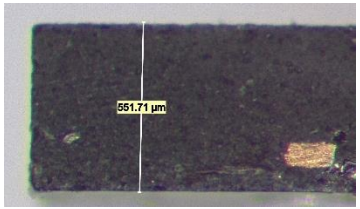


Same number

Shape of pin 1 mark

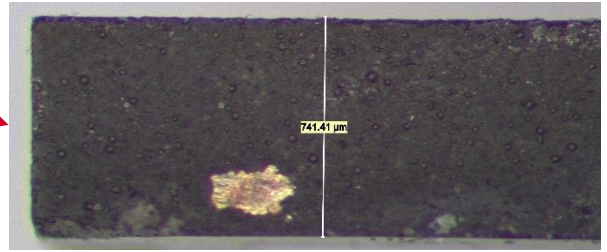


Lighter font



Old gen OEM

Thicker package



Third party

IOActive.

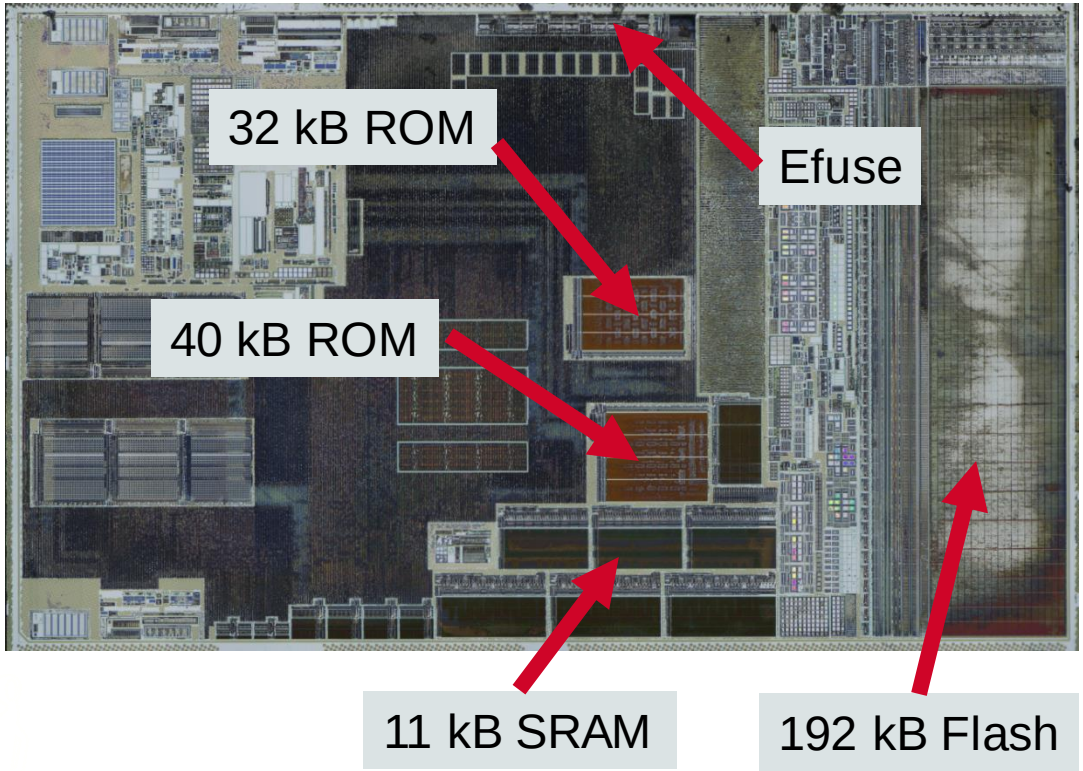
Why so similar?

- They're not "counterfeits"
  - No chance of tricking the OEM into buying this

Why so similar?

- They're not "counterfeits"
  - No chance of tricking the OEM into buying this
- Working theory: Fourth party pwned OEM chipset
  - They want royalties on the clone market
  - Sell pre-keyed SE's to unlicensed accessory vendors
  - Use similar markings so prospective buyers recognize it

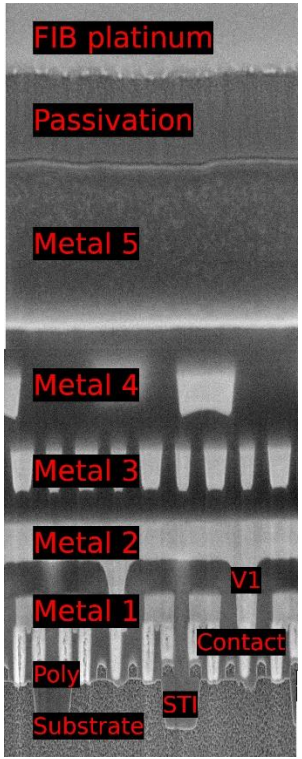
Old gen OEM: secure element

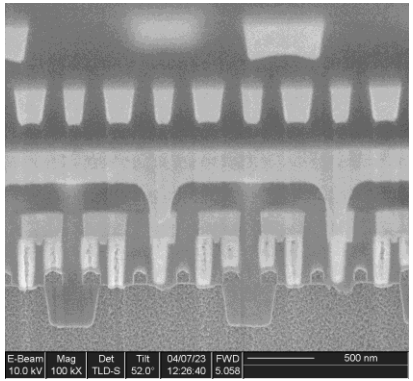


- 3.42 mm^2
- 90 nm
- BEOL: 4 Cu + 1 Al
- ≈ 475 kGate

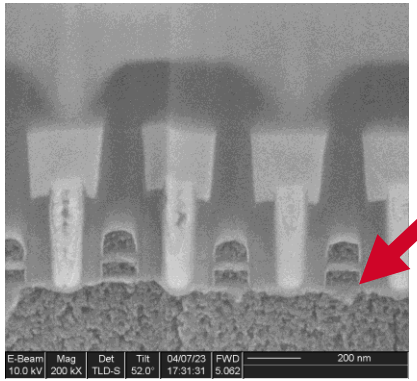
IOActive.

Old gen OEM SE: Cross section



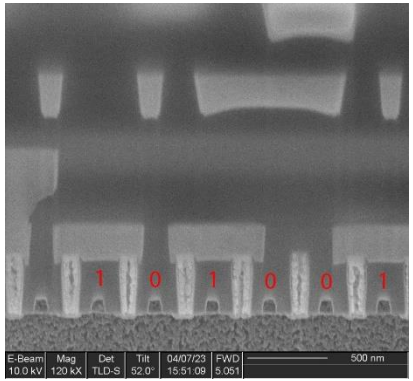


SRAM PMOS



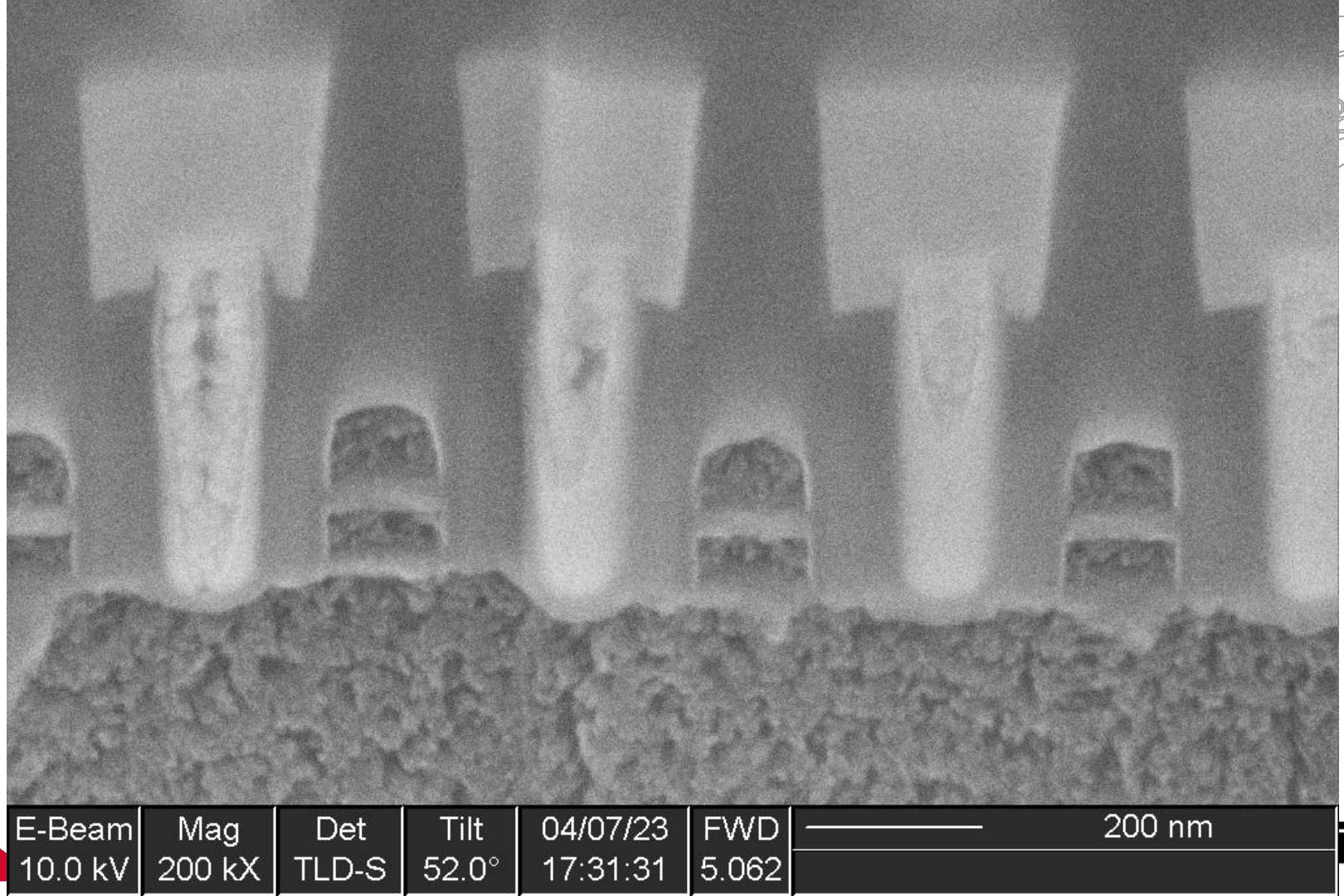
Flash

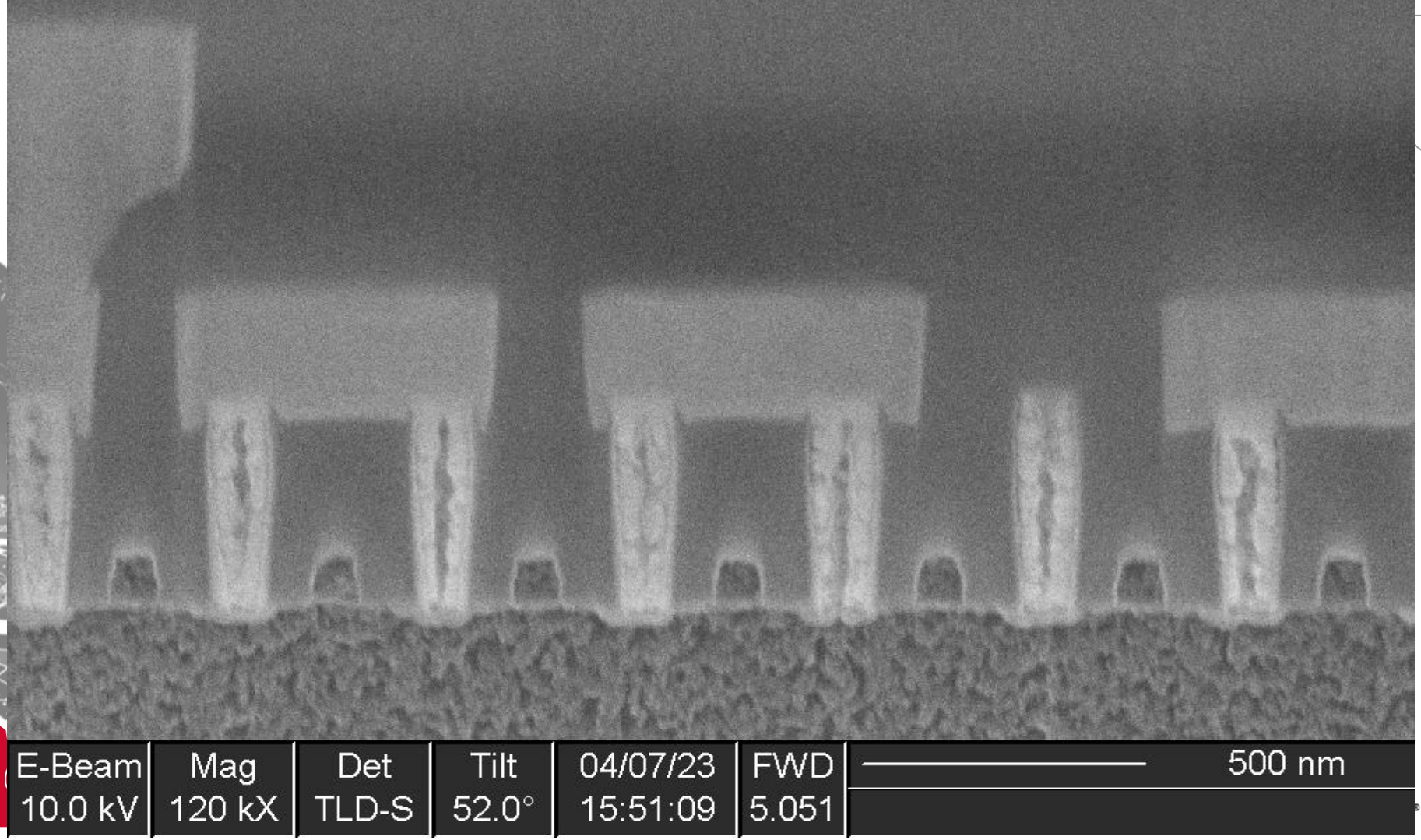
Floating gates

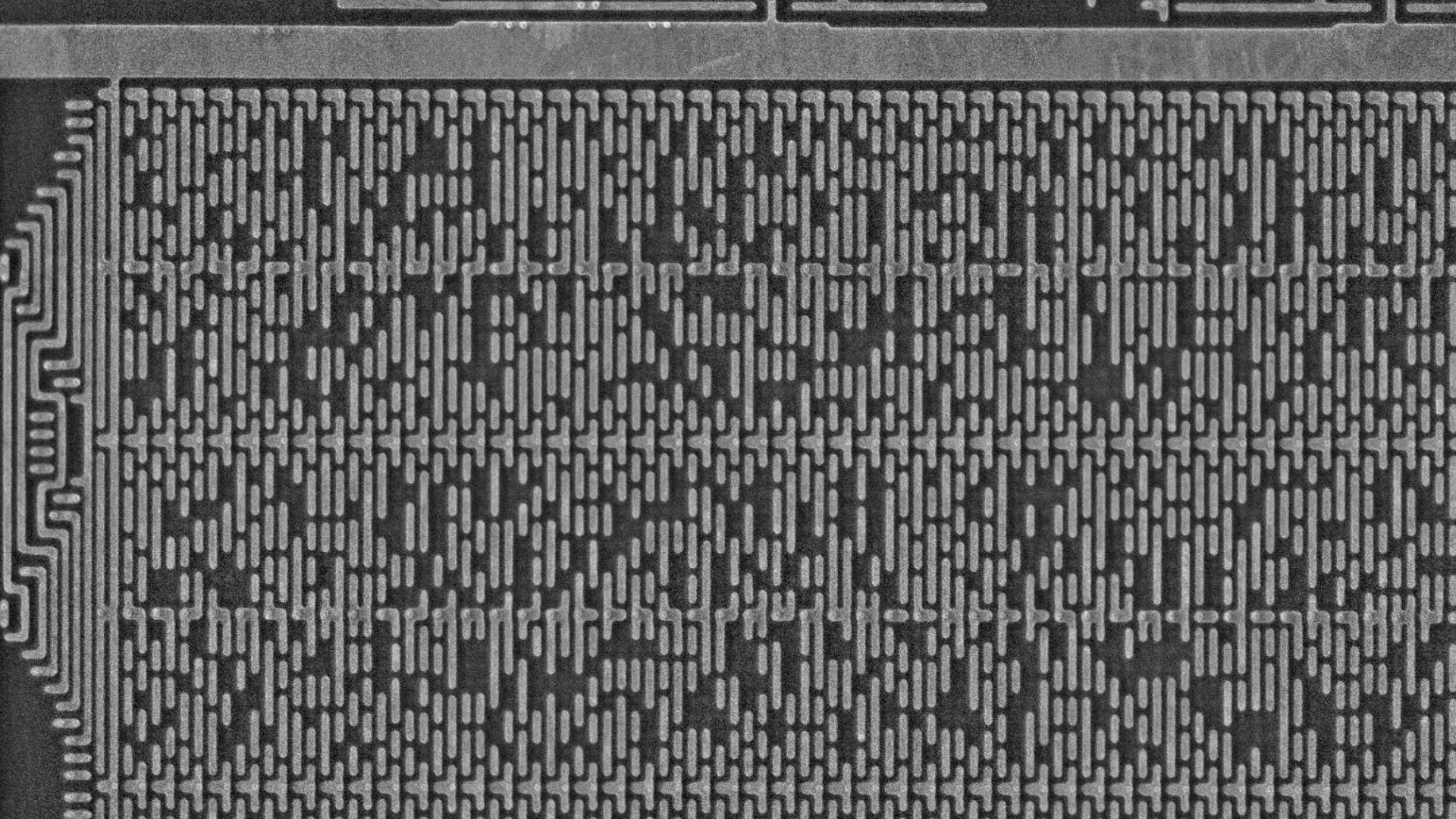


ROM

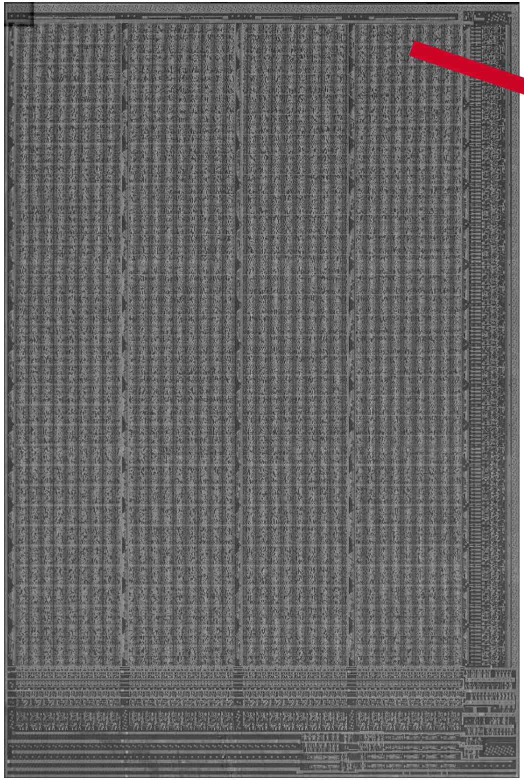
IOActive.

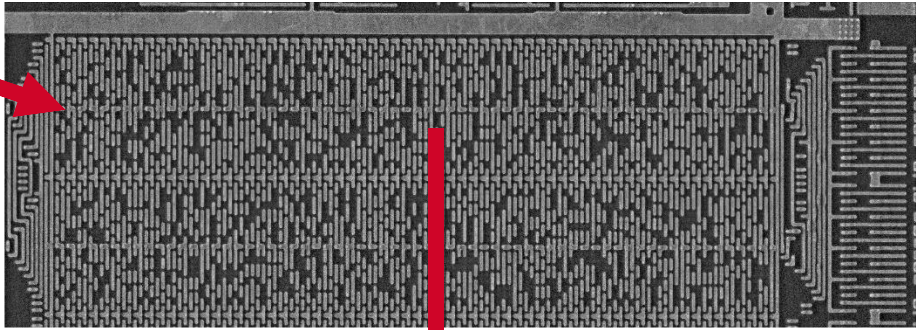

E-Beam
10.0 kV
Mag
200 kX
Det
TLD-S
Tilt
52.0°
04/07/23
17:31:31
FWD
5.062
200 nm


E-Beam
10.0 kV
Mag
120 kX
Det
TLD-S
Tilt
52.0°
04/07/23
15:51:09
FWD
5.051
500 nm



Old gen OEM SE: M1 ROM extraction

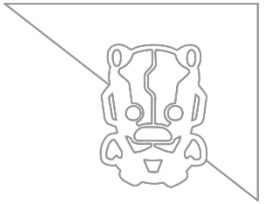




00011111101010001101100100110110101110101001101010100110010000111001001101110010101101010110100011011000011011001110011101100101
0111110001111010111100011001111111001100101000010111000111111100010110000001001010011111101011001010001000111101011011101011101
1001110110100011010000000011101111010101111010010101111011000111010101101110110111001110101110111000100110001110001110000111100
1011001110101011101011110111110011010010100011010100011000100101011110101010100110100001010010000010111011101101100100100110111
0000110011111001100010000011101101011100001011111001101100111010000100100111110110001111001011101000011001100001000011111010111
11101101010111010100001011001000110100010000100010111010110010101011101101101100100101101110110101111111000001100110011011101001
11011000001001110101101110010011100100010100010111101110110110100110101100010001010110000110011100110010011011100100111110011
101001110100110100111110101100111001000010100110010011100100001011011110101001110110001001010001110110000100011101010010000011
0011100110101111011100101000100001101111000011011100011001111001111001000001111001010100000100101011001010001111000011100000001
10010100011011100000000001000011010001010000011011111101011100000100101111101111011111000010101100010010101010111011110111001010
01011011101110100101100100110010111100010100011101011000110001001111001111100001110010101101101110001111000110100110011010001010
001100011100000010011011100010111101001111110111100000000011010011101101101110110100101000001001000000101011111100000010001000
110001110111000000111111101100001011110000000100001100010111000100001101010000000010100100100111010000000100111101111101101011110
1101001110000111011010100000111101110010100111110000010001011100111100010001110011101110100001100011001110110000010101011010000
000101011101001010000111000111111100000001011000011111111001111000000010100111011000011110101100101011110001111011101010001001
00010110010100001101101111011100110111010000100010001001101000111101000010010011100111010001010001101100010001101100010110110010

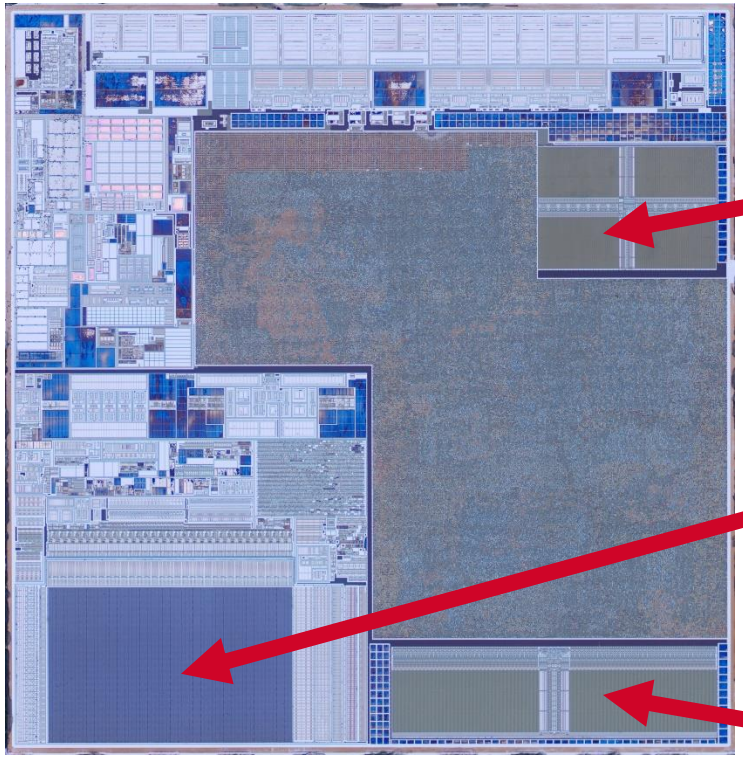
IOActive.

Old gen OEM SE: M1 ROM



- It’s encrypted ☹
- Didn’t find/reverse decryption logic
- Likely not how the cloner got in

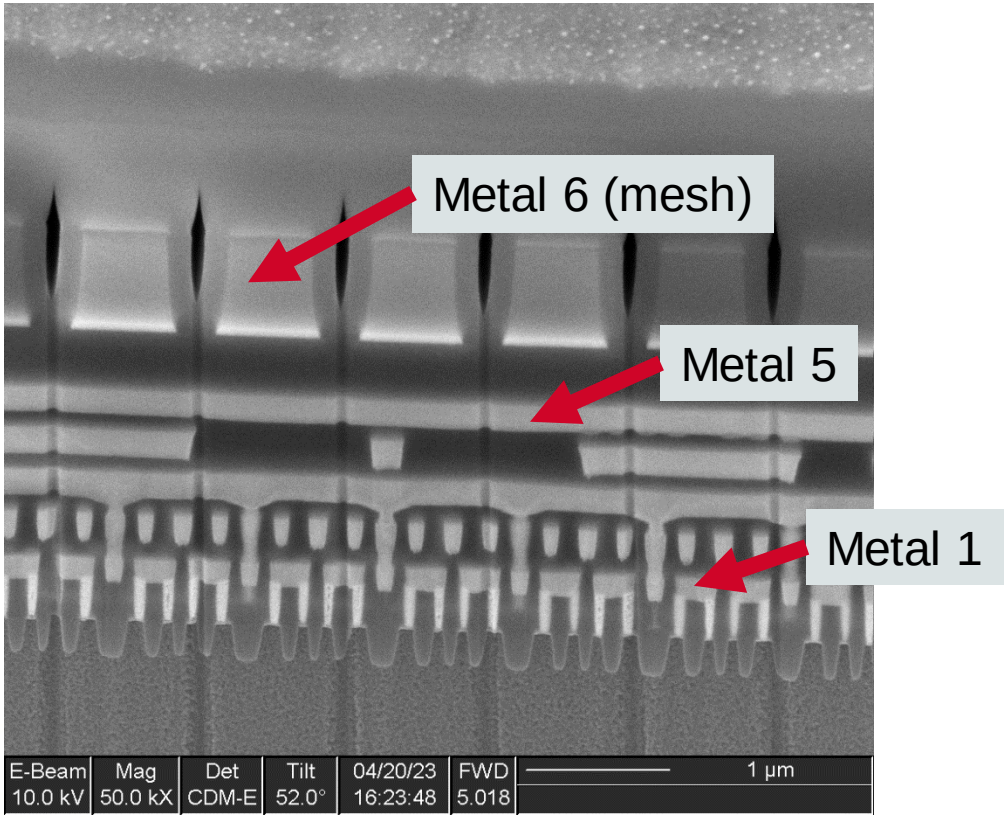
Third party: secure element

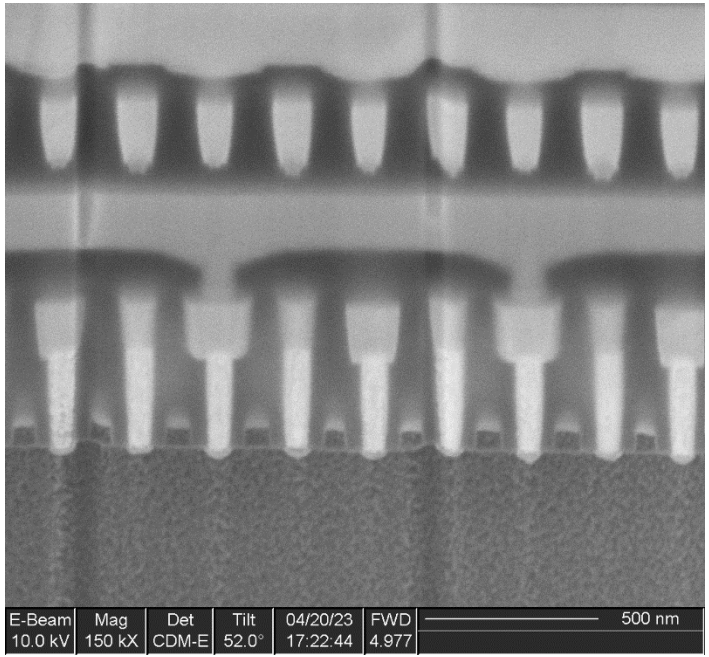


- 1.28 mm^2
- 55 nm
- BEOL: 5 Cu + 1 Al
- ≈ 450 kGate

IOActive.

Third party secure element



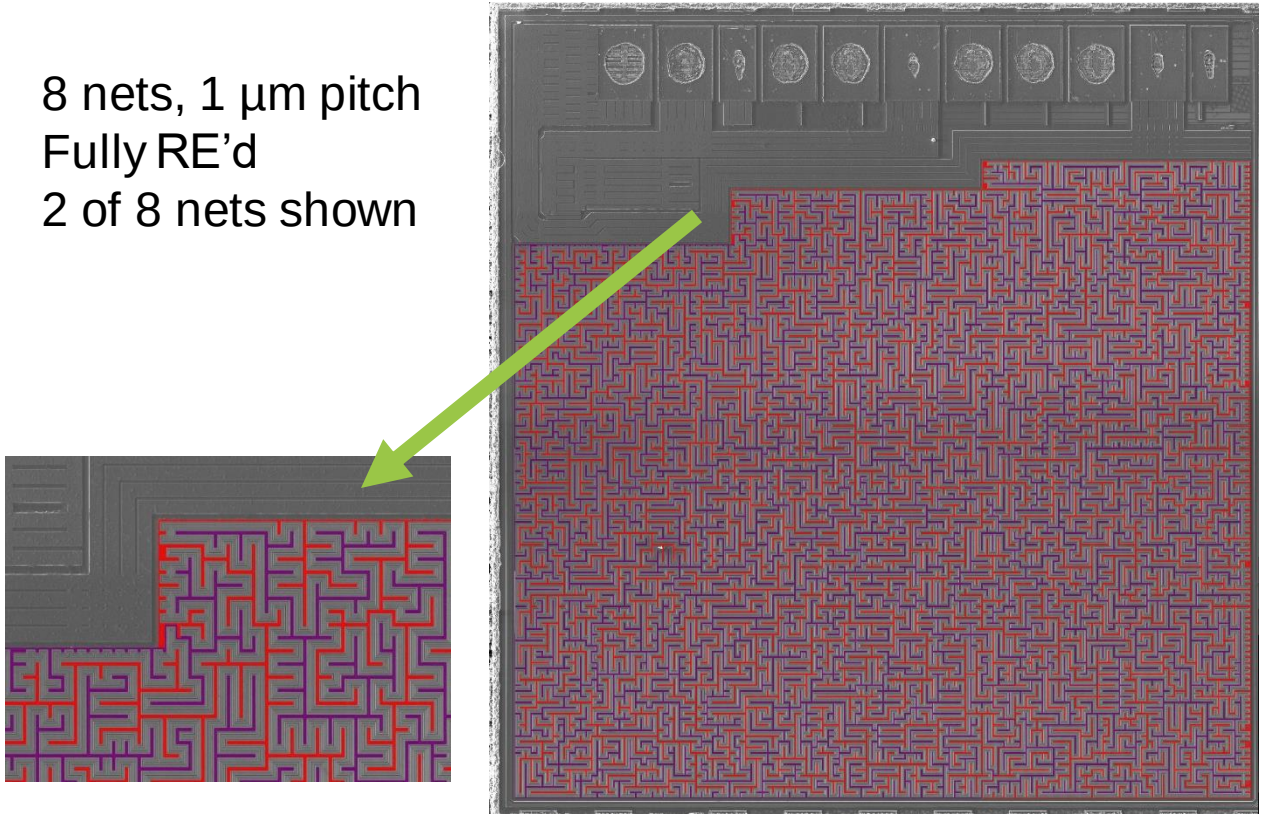


SRAM NMOS

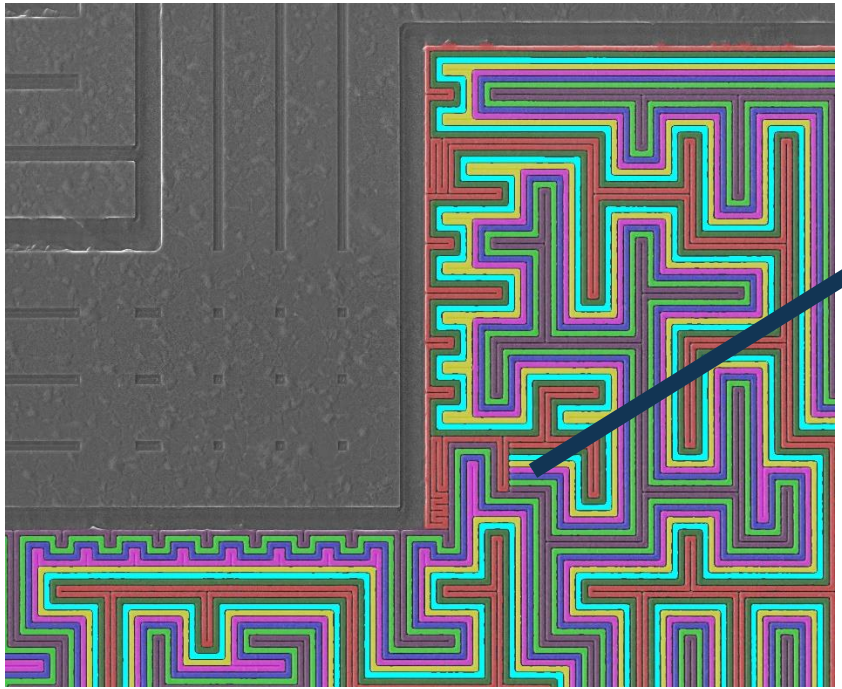
IOActive.

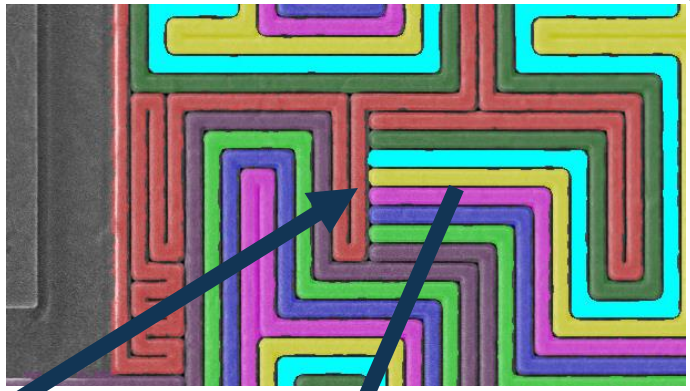
Third party secure element: Active mesh

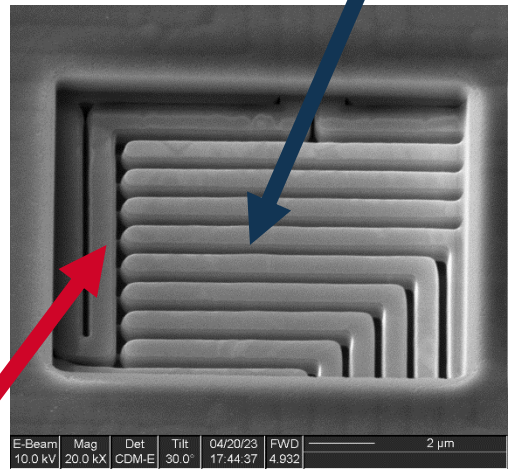
- 8 nets, 1 µm pitch
- Fully RE'd
- 2 of 8 nets shown



Security mesh tracing



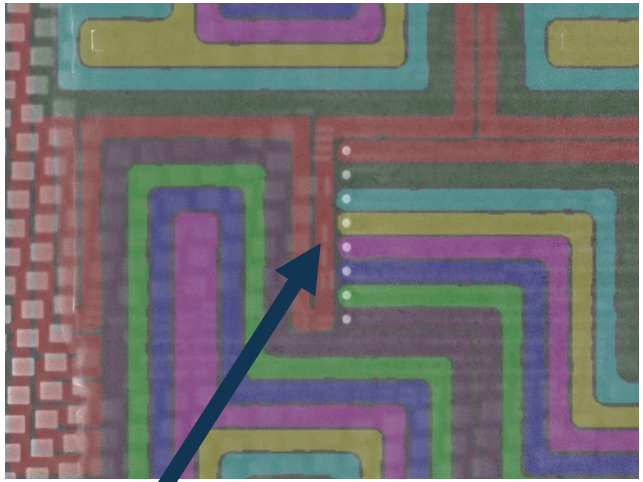




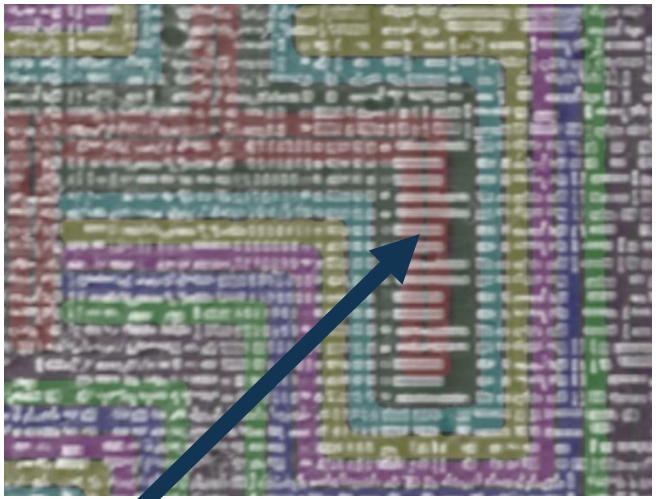
Mesh end

IOActive.

Security mesh drive logic



Vias to M5



8x high drive buffer cells

Overall conclusions

- OEM redesign introduced a weakness
  - Rapidly exploited by cloners
  - SPI flash probably contains the private key
- Original OEM design likely undefeated
- Cloners don’t like competition

Questions?