Die Hard 7: Passwords Plz

Extracting secrets from hardware

Intro to the talk

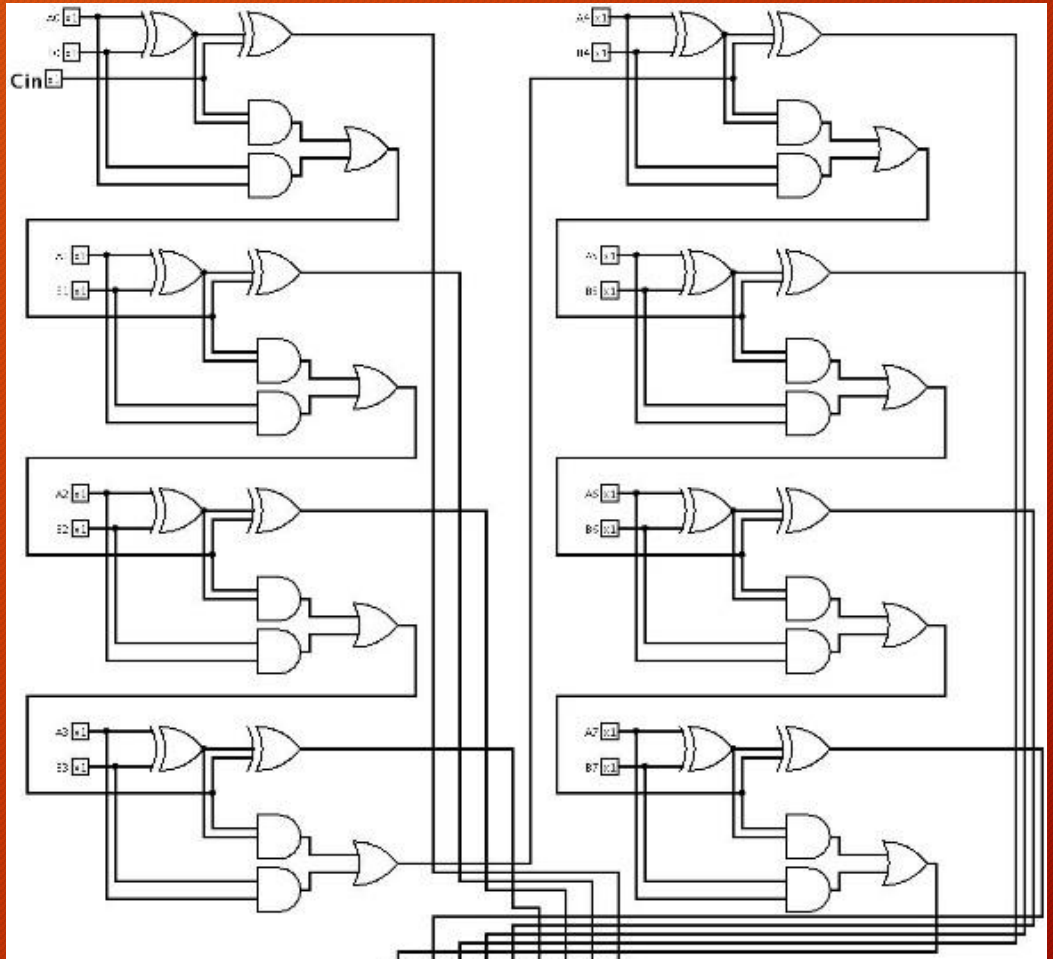
- No time for $whoami!
- How to make a chip
- How to break a chip
- ~~Demo~~
- How to protect a chip
- Fin

Physical Security Matters

Define the chip and describe it

VHDL Code

```
-- Here we define the AND gate that we need for
-- the Half Adder
library ieee;
use ieee.std_logic_1164.all;

entity andGate is
  port( A, B : in std_logic;
        F : out std_logic);
end andGate;

architecture func of andGate is
begin
  F <= A and B;
end func;
--*============================

-- Here we define the XOR gate that we need for
-- the Half Adder
library ieee;
use ieee.std_logic_1164.all;

entity xorGate is
  port(  A, B : in std_logic;
        F : out std_logic);
end xorGate;
```

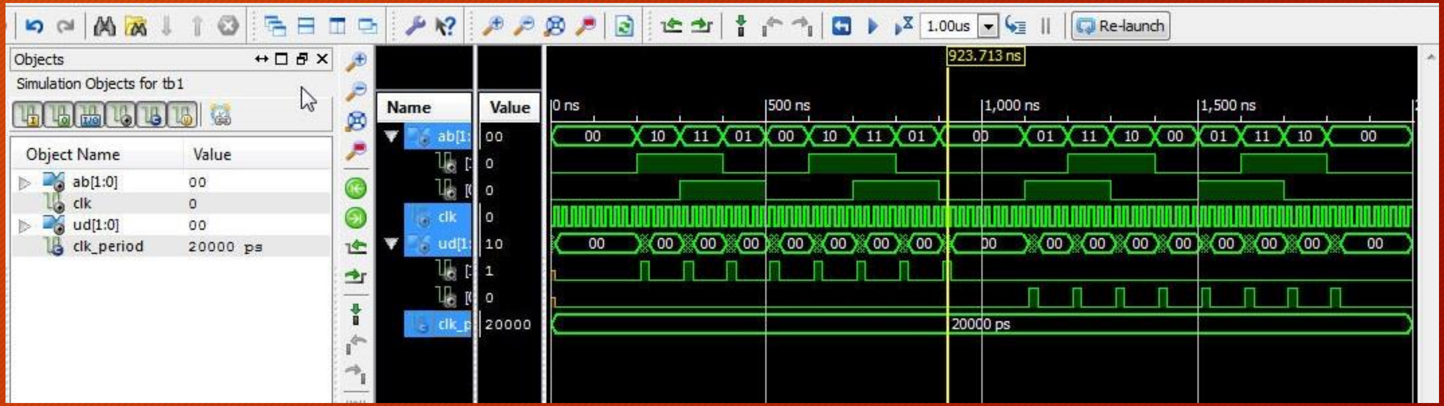


Simulate the design and timings

VHDL Test Bench

```
--import std_logic from the IEEE library
library ieee;
use ieee.std_logic_1164.all;

entity fullAdder_tb is
end fullAdder_tb;

architecture tb of fullAdder_tb is

   component fullAdder is
      port( A, B, Cin : in std_logic;
            sum, Cout : out std_logic);
   end component;

   signal A, B, Cin, sum, Cout : std_logic;
```

Timing Simulation



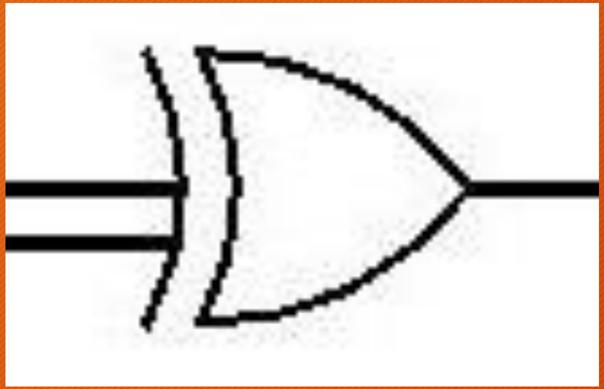
Objects

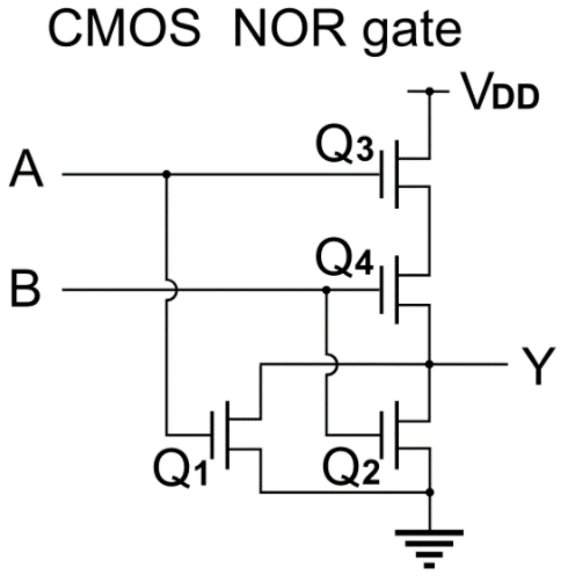
Simulation Objects for tb1

Object Name	Value
ab[1:0]	00
clk	0
ud[1:0]	00
clk_period	20000 ps

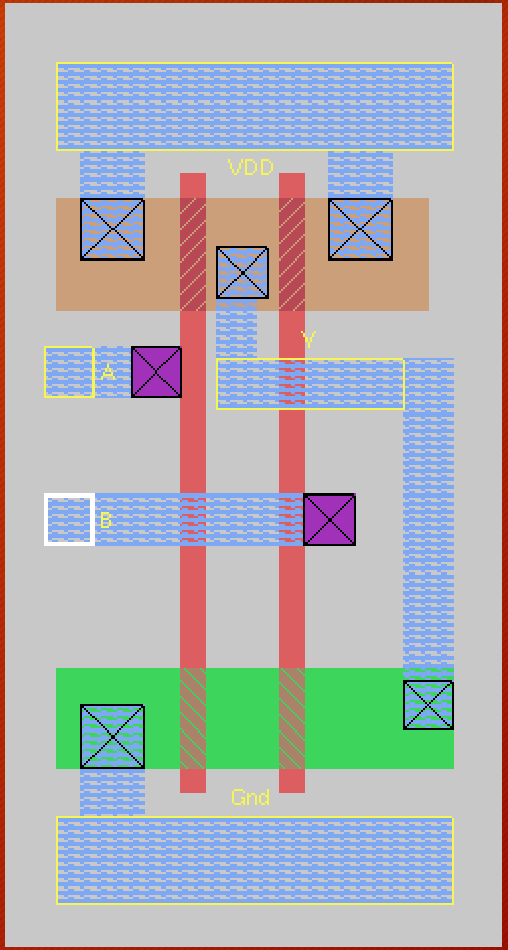
Name	Value
ab[1:	00
[	0
[(	0
clk	0
ud[1:	10
[	1
[(	0
clk_p	20000

Break each functional part into standard blocks

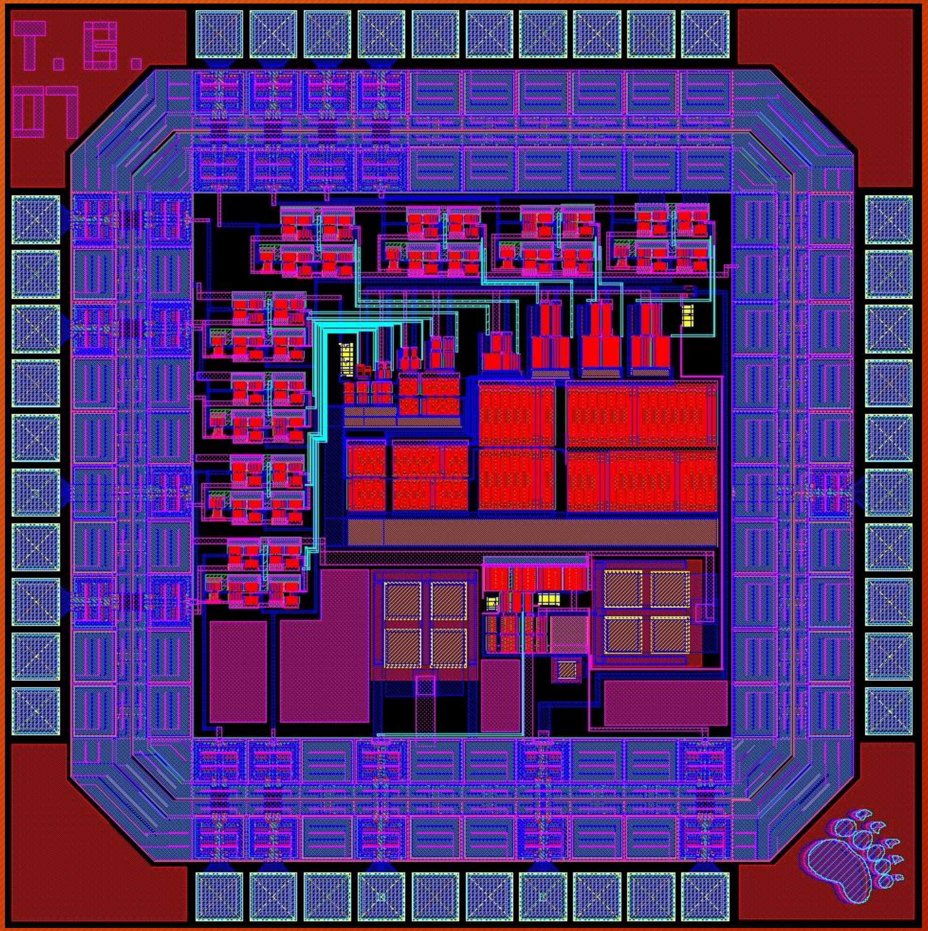




CMOS NOR gate



Join the blocks and create the chip layout

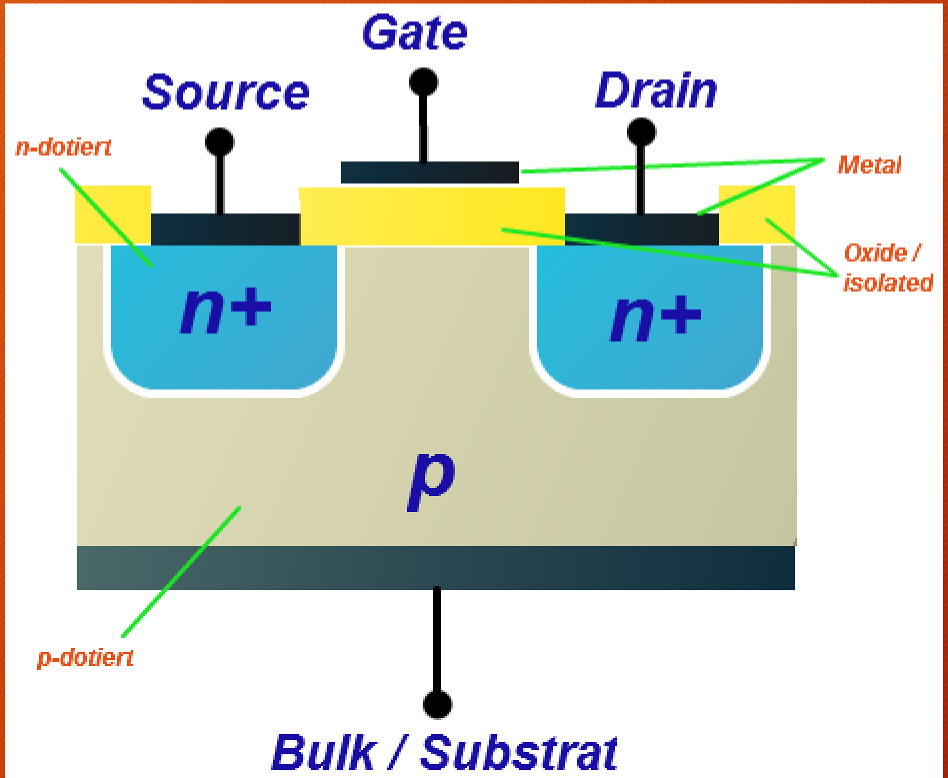


http://web.eece.maine.edu/research/vlsi/2007/Bellamine/

Get Sand (like, really pure sand)

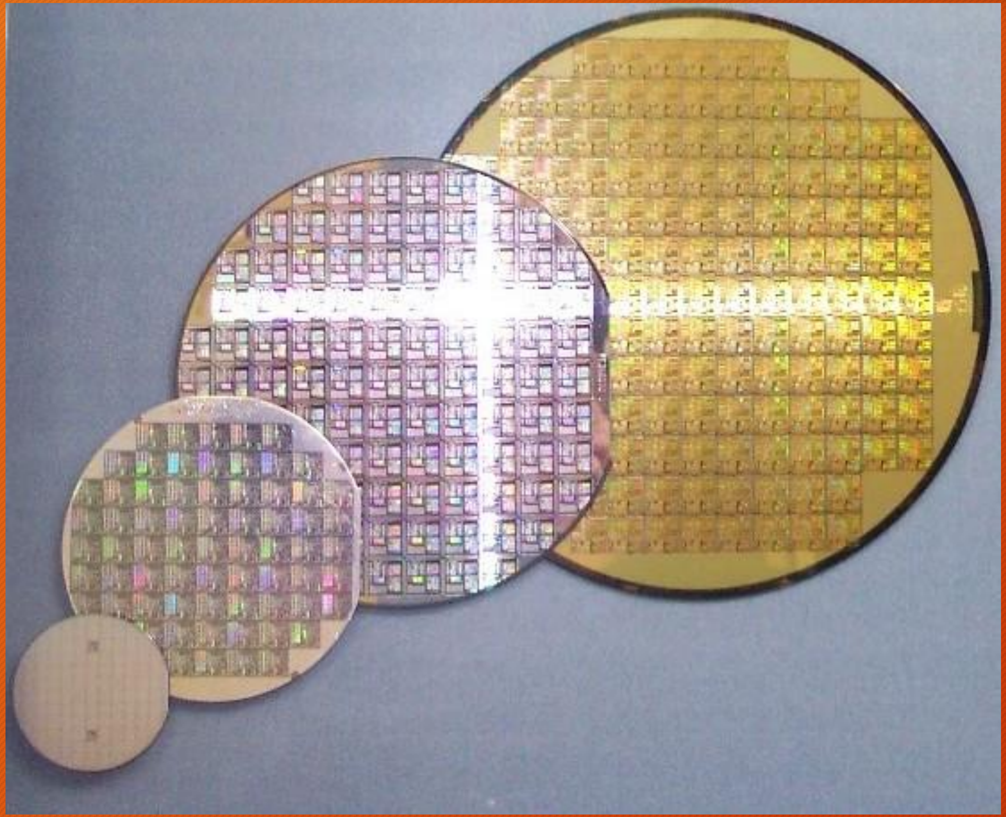
Get the chip doped up and metalled \o/

Get the chip doped up and metalled \o/

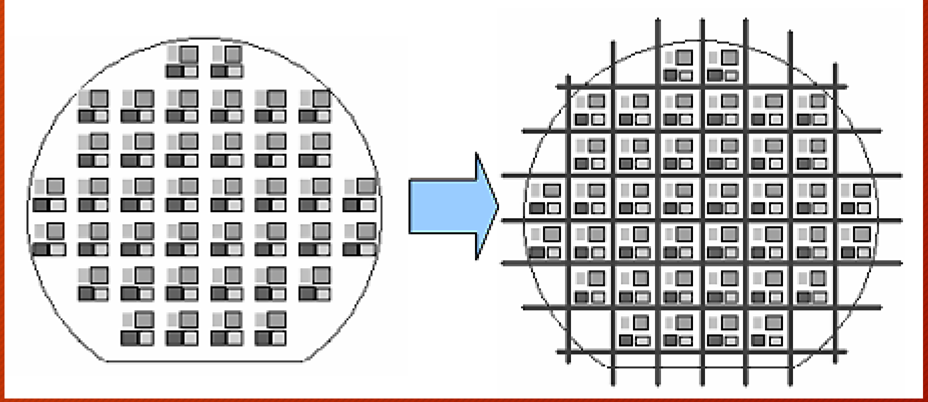


http://images.tutorvista.com/cms/images/81/metal-oxide-semiconducto.png

Slice and Dice

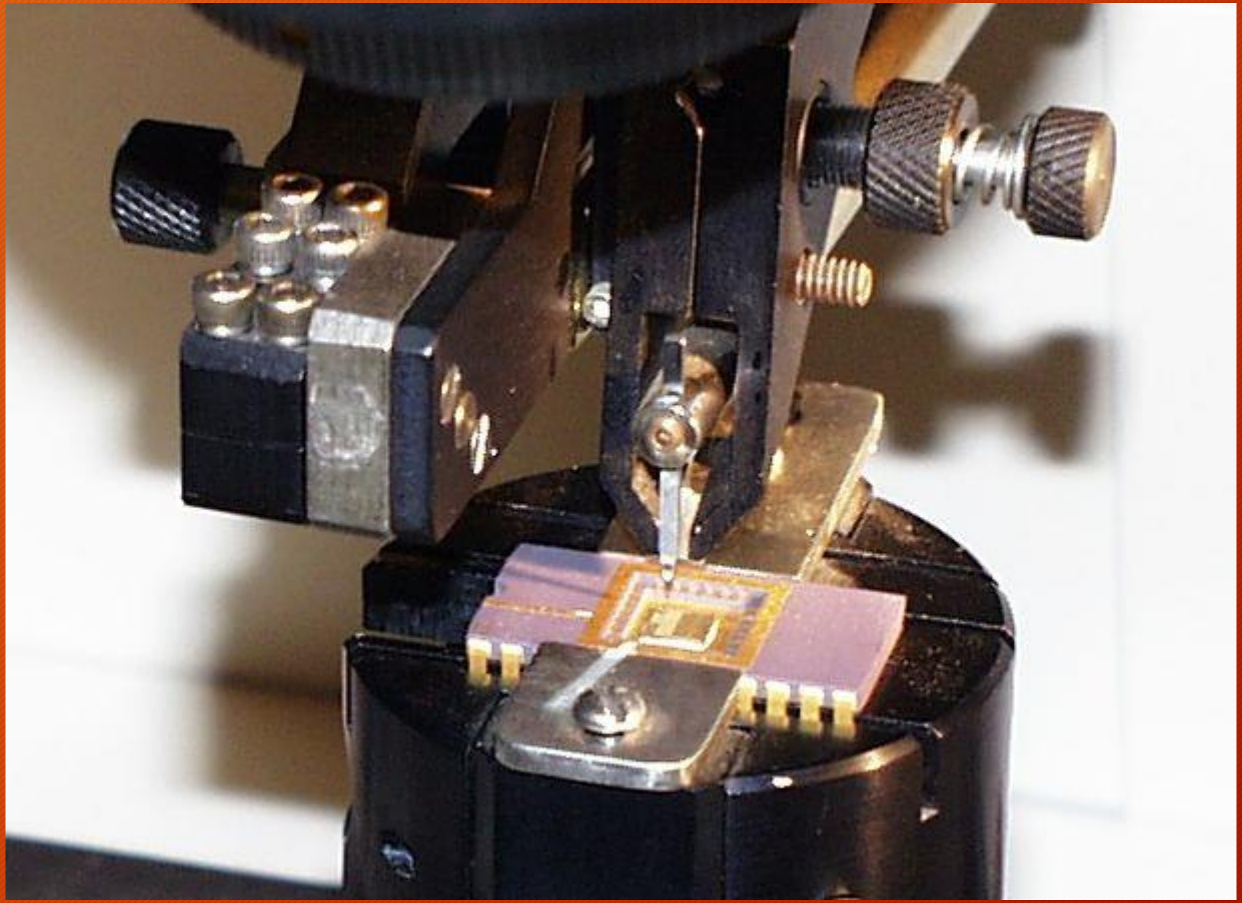


https://upload.wikimedia.org/wikipedia/commons/d/d7/Wafer_2_Zoll_bis_8_Zoll_2.jpg



http://electronics.stackexchange.com/questions/42765/orientaion-flat-on-semiconductor-wafer

Bond out the wires into the chosen package



Package and Sell, Sell, Sell!

http://www.soselectronic.com/a_info/img_data/Taiwan_Semiconductor/reel.jpg

So why did I go through this

- ~~Because it makes me feel like a real man~~
- You need to know how a chip is constructed to then attack it effectively.
- Identifying common structures in a chip allows you to reverse its functionality.
- And knowing these structures allow you to identify areas to attack

Reversing a silicon chip

Step 1. Get samples to research!

Digi-Key®
CORPORATION

MOUSER
ELECTRONICS

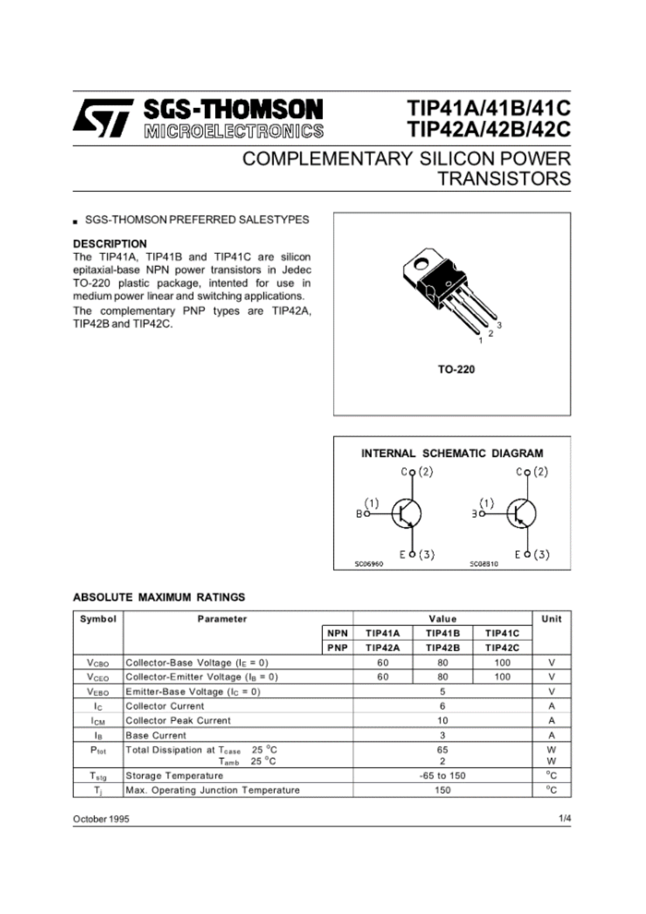
Farnell

淘宝网
Taobao.com

ebay

Alibaba Group
阿里巴巴集团

Get all the infos needed for the chip.



SGS-THOMSON
MICROELECTRONICS

TIP41A/41B/41C
TIP42A/42B/42C

COMPLEMENTARY SILICON POWER TRANSISTORS

- SGS-THOMSON PREFERRED SALESTYPES

DESCRIPTION
The TIP41A, TIP41B and TIP41C are silicon epitaxial-base NPN power transistors in Jedec TO-220 plastic package, intented for use in medium power linear and switching applications.
The complementary PNP types are TIP42A, TIP42B and TIP42C.

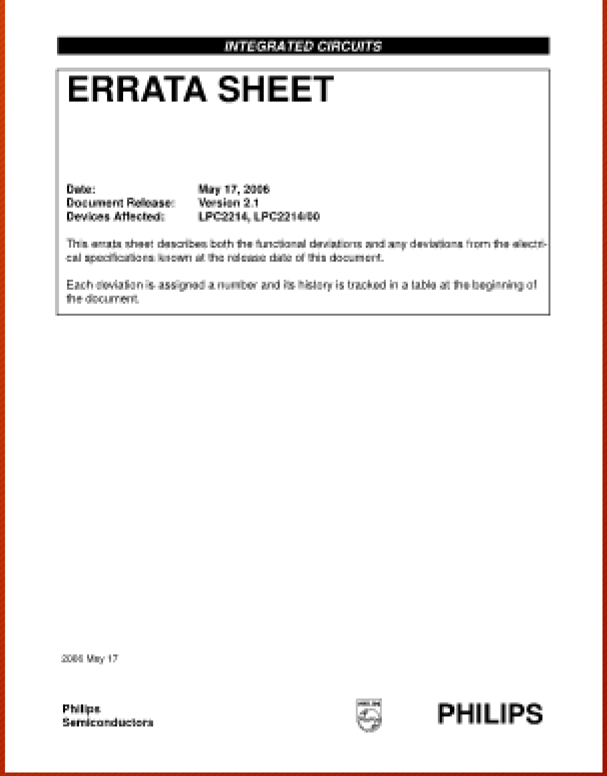
TO-220

INTERNAL SCHEMATIC DIAGRAM

ABSOLUTE MAXIMUM RATINGS

Symbol	Parameter		Value			Unit
		NPN	TIP41A	TIP41B	TIP41C	
		PNP	TIP42A	TIP42B	TIP42C	
V_{CBO}	Collector-Base Voltage (I_E = 0)		60	80	100	V
V_{CEO}	Collector-Emitter Voltage (I_B = 0)		60	80	100	V
V_{EBO}	Emitter-Base Voltage (I_C = 0)		5			V
I_C	Collector Current		6			A
I_{CM}	Collector Peak Current		10			A
I_B	Base Current		3			A
P_{tot}	Total Dissipation at T_{case} 25 °C T_{amb} 25 °C		65 2			W W
T_{stg}	Storage Temperature		-65 to 150			°C
T_j	Max. Operating Junction Temperature		150			°C

October 1995 1/4



INTEGRATED CIRCUITS

ERRATA SHEET

Date:	May 17, 2006
Document Release:	Version 2.1
Devices Affected:	LPC2214, LPC2214/00

This errata sheet describes both the functional deviations and any deviations from the electrical specifications known at the release date of this document.

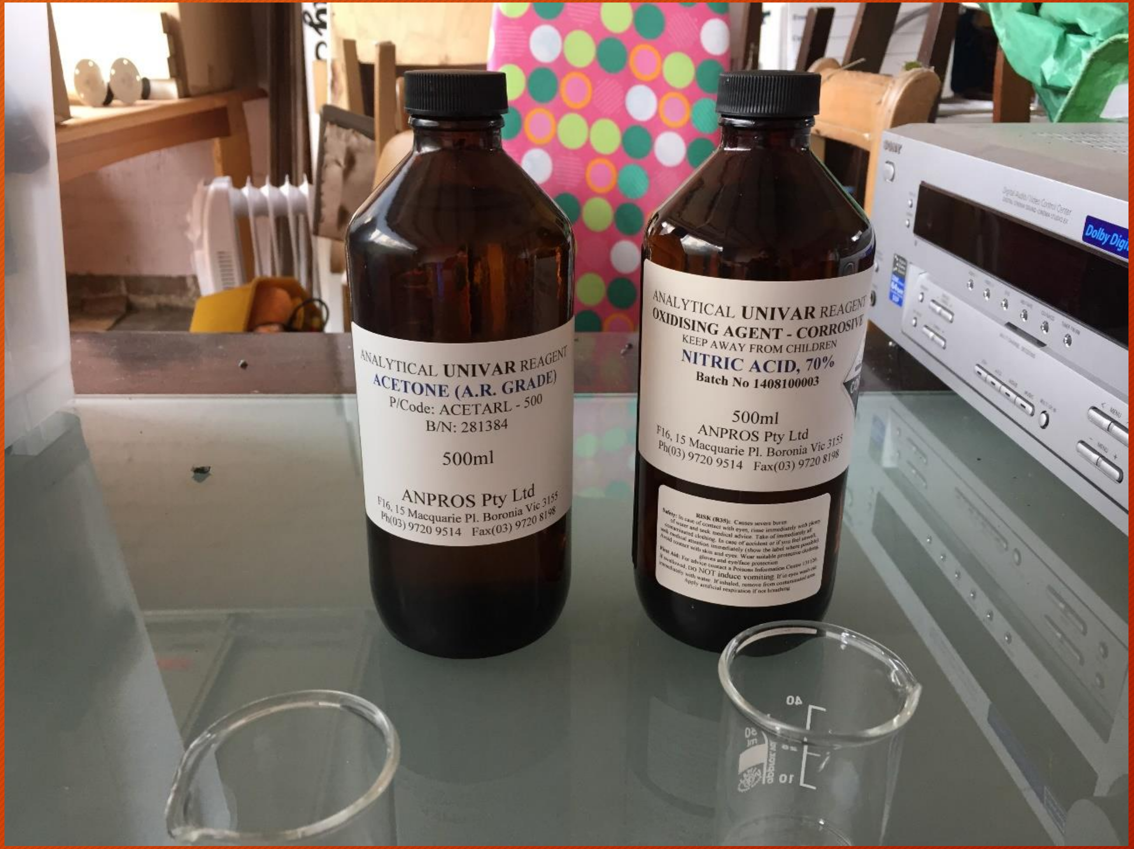
Each deviation is assigned a number and its history is tracked in a table at the beginning of the document.

2006 May 17

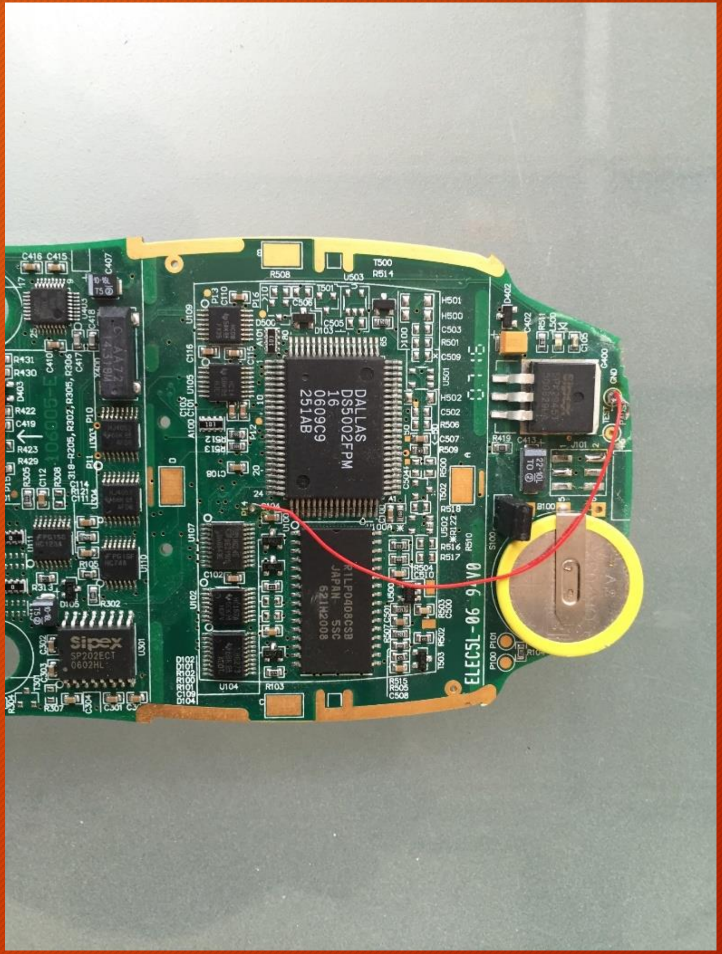
Philips
Semiconductors

PHILIPS

Decapsulate (decap) the chip!


ANALYTICAL UNIVAR REAGENT
ACETONE (A.R. GRADE)
P/Code: ACETARL - 500
B/N: 281384
500ml
ANPROS Pty Ltd
F16, 15 Macquarie Pl. Boronia Vic 3155
Ph(03) 9720 9514 Fax(03) 9720 8198
ANALYTICAL UNIVAR REAGENT
OXIDISING AGENT - CORROSIVE
KEEP AWAY FROM CHILDREN
NITRIC ACID, 70%
Batch No 1408100003
500ml
ANPROS Pty Ltd
F16, 15 Macquarie Pl. Boronia Vic 3155
Ph(03) 9720 9514 Fax(03) 9720 8198
40
10

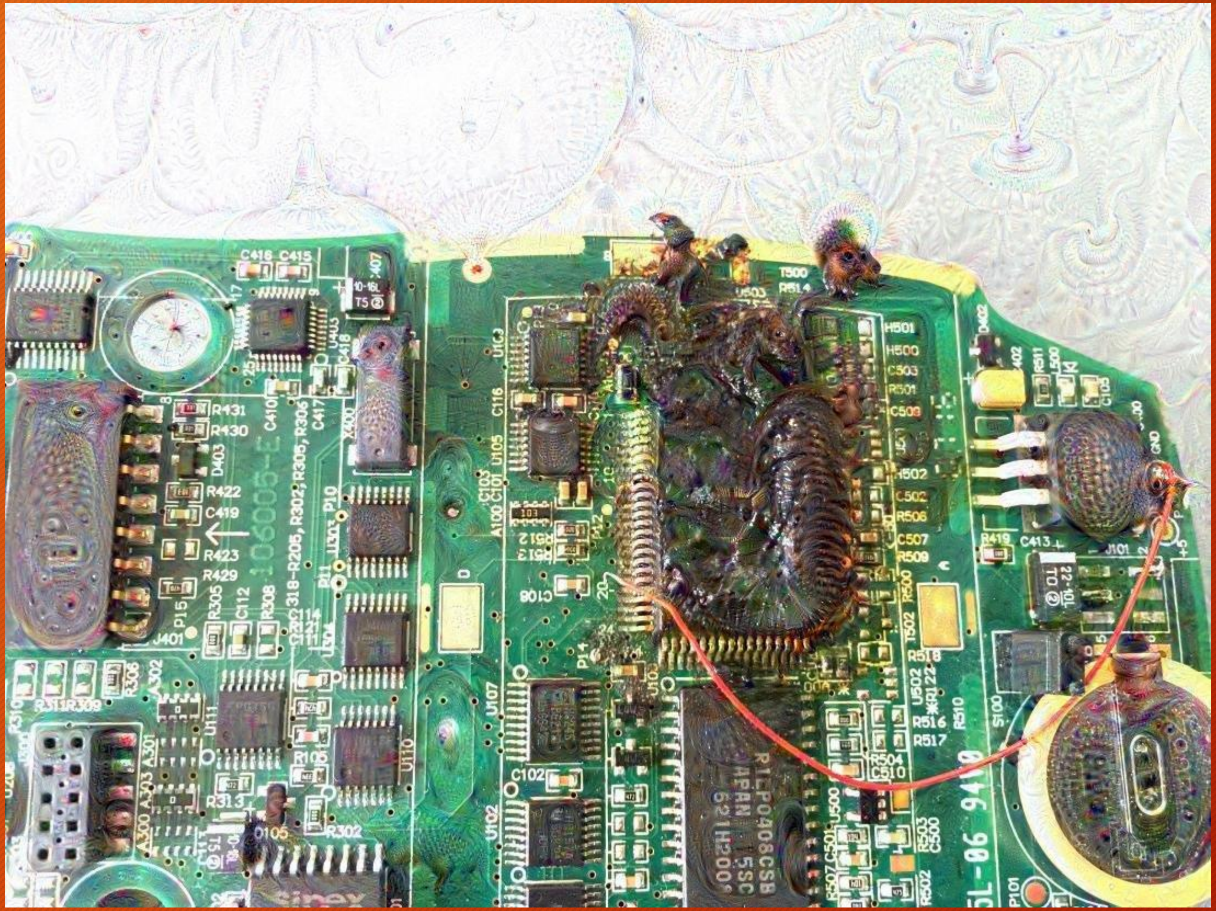
Look a chip – look at it.



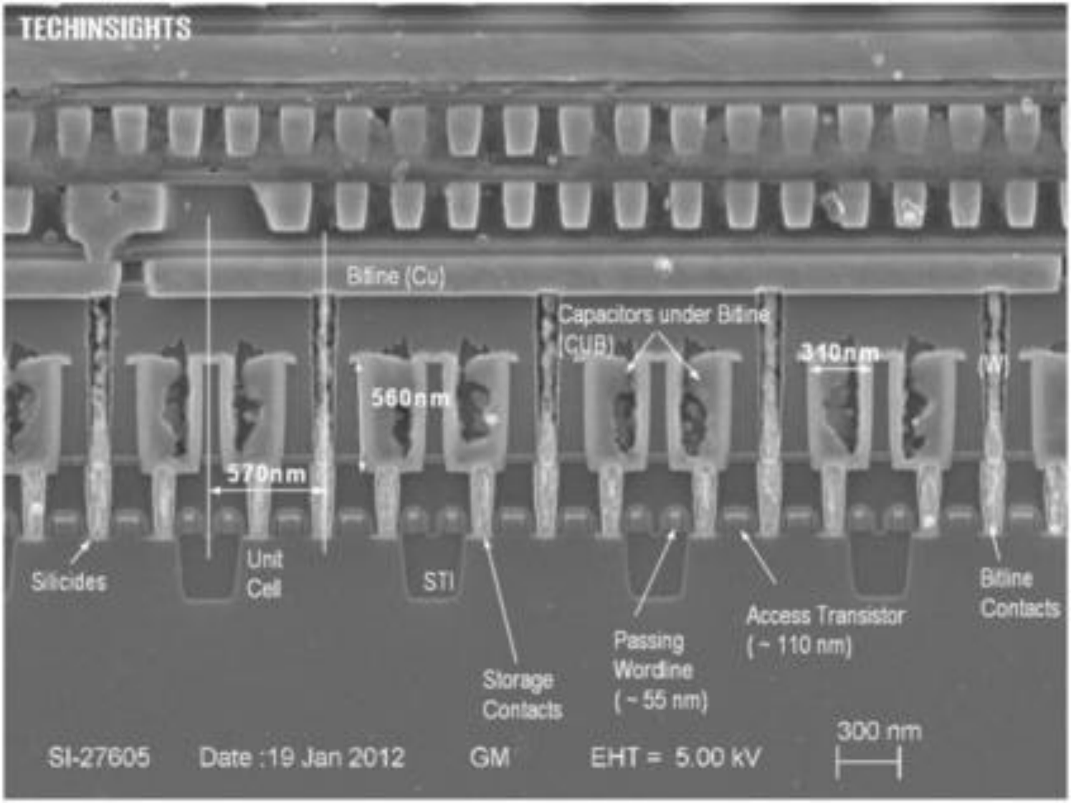
Safety is important*

*maybe not that safe…

Don’t inhale deeply… (snare)

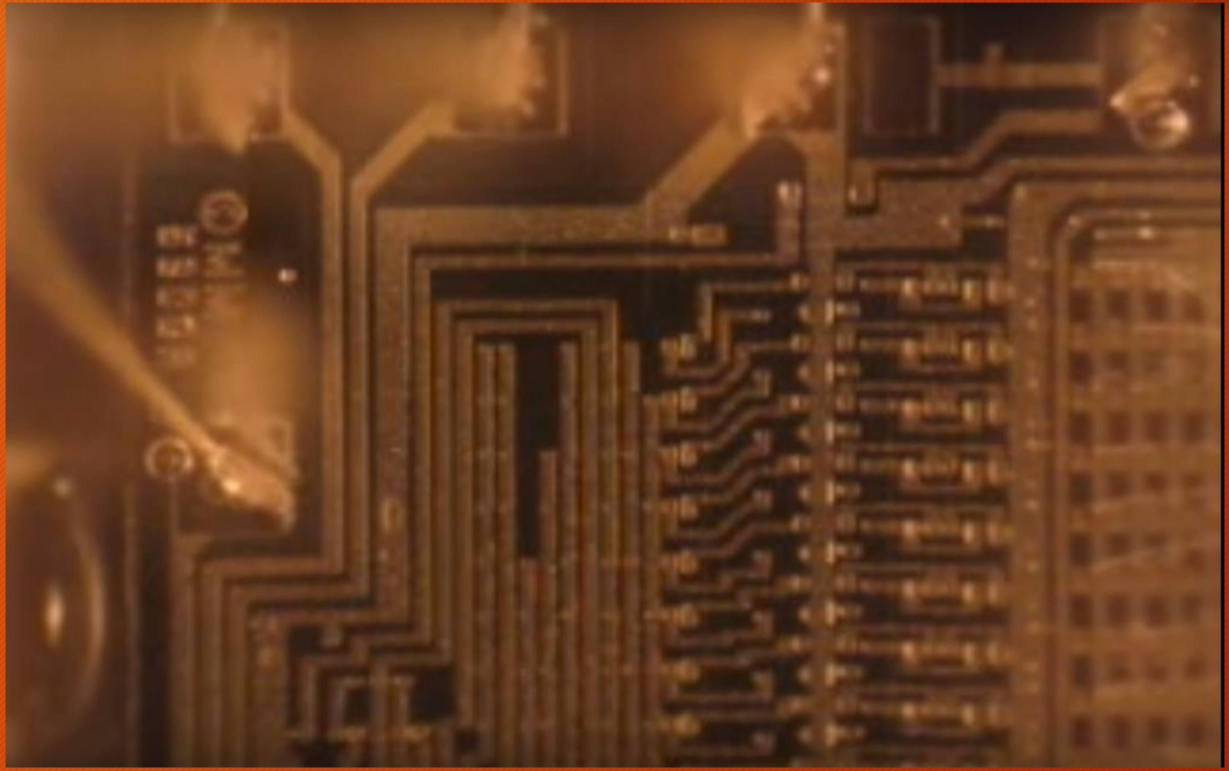


Use Scanning Electron Microscope to work out how many metal layers the chip has



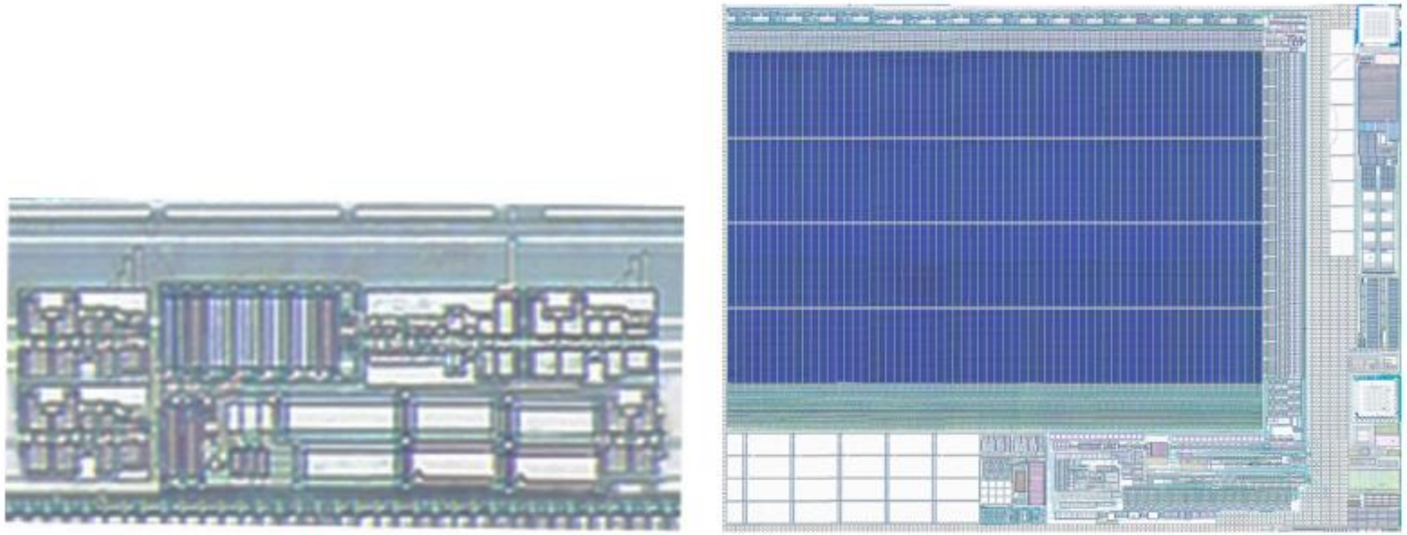
http://m.eet.com/media/1158119/120420_techinishgts1.jpg

Dissolve each layer using scary stuff and image using high resolutions



John McMaster is awesome – watch this: https://www.youtube.com/watch?v=ZKT2Giq-lbQ

Stitch it together using geo-mapping software.

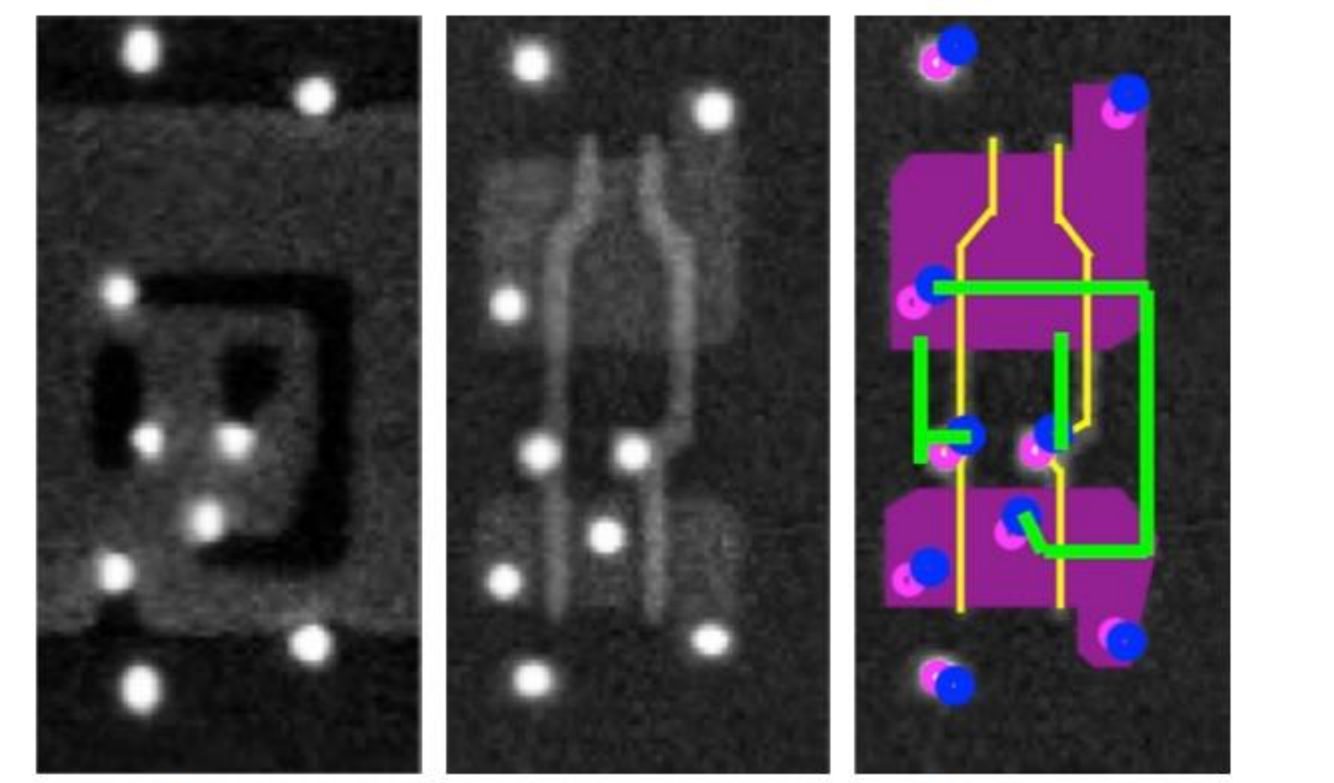


(a) Single flash buffer.

(b) Layout of the flash memory.

Image courtesy Olivier THOMAS @ Texplained
Dmitry Nedospasov (@nedos on the twitter)
http://www.texplained.com/

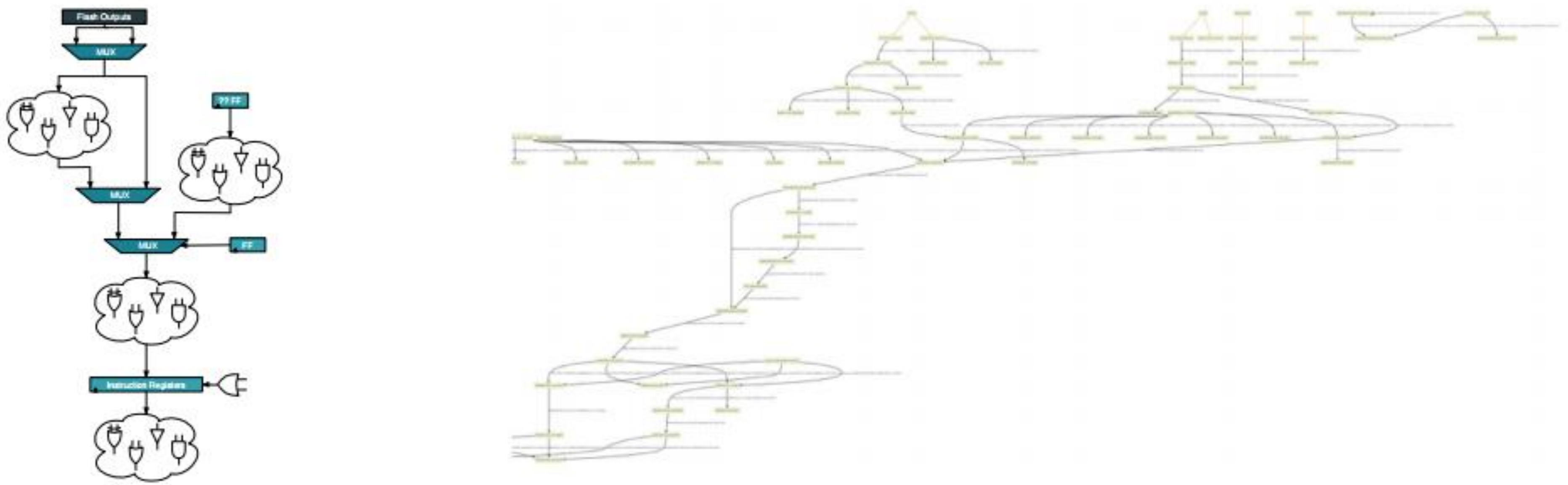
Identify the components



(a) Source Image (b) Detected Interconnects (c) Detected Interconnects

Olivier THOMAS Texplained
Dmitry Nedospasov
http://www.texplained.com/

Reconstruct the circuit



(a) Data path schematic.

(b) ARES graph tracing.

Olivier THOMAS Texplained
Dmitry Nedospasov
http://www.texplained.com/

Image the ROM and read of – if the chip is >40uM size (i.e from the 90's)

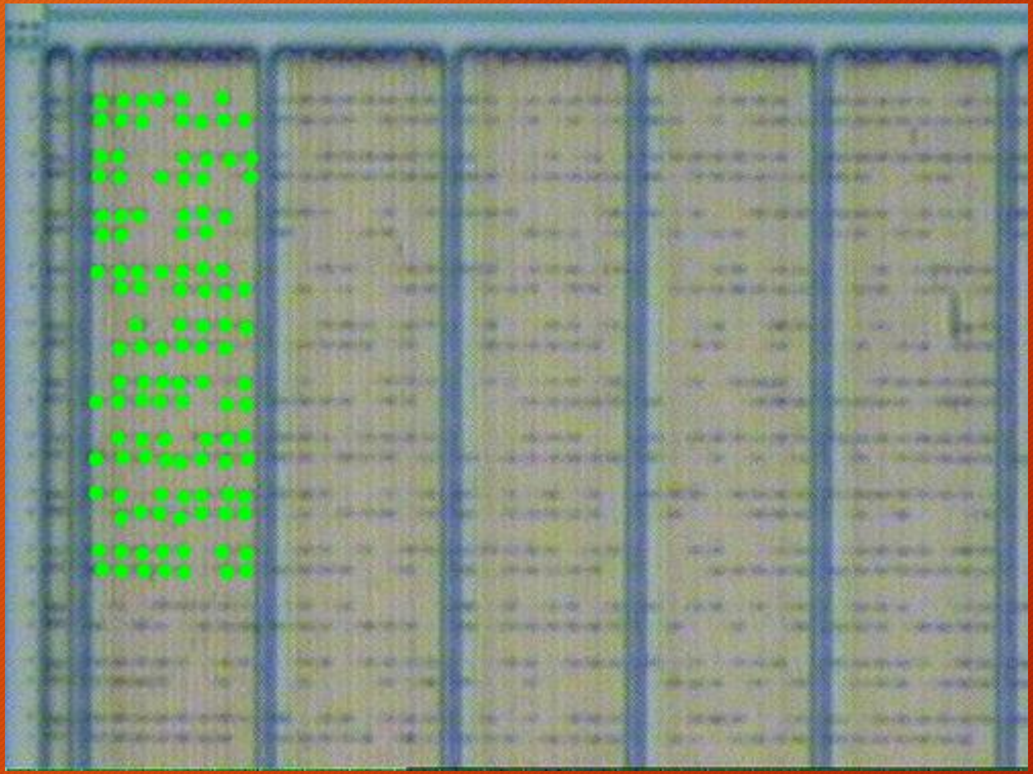
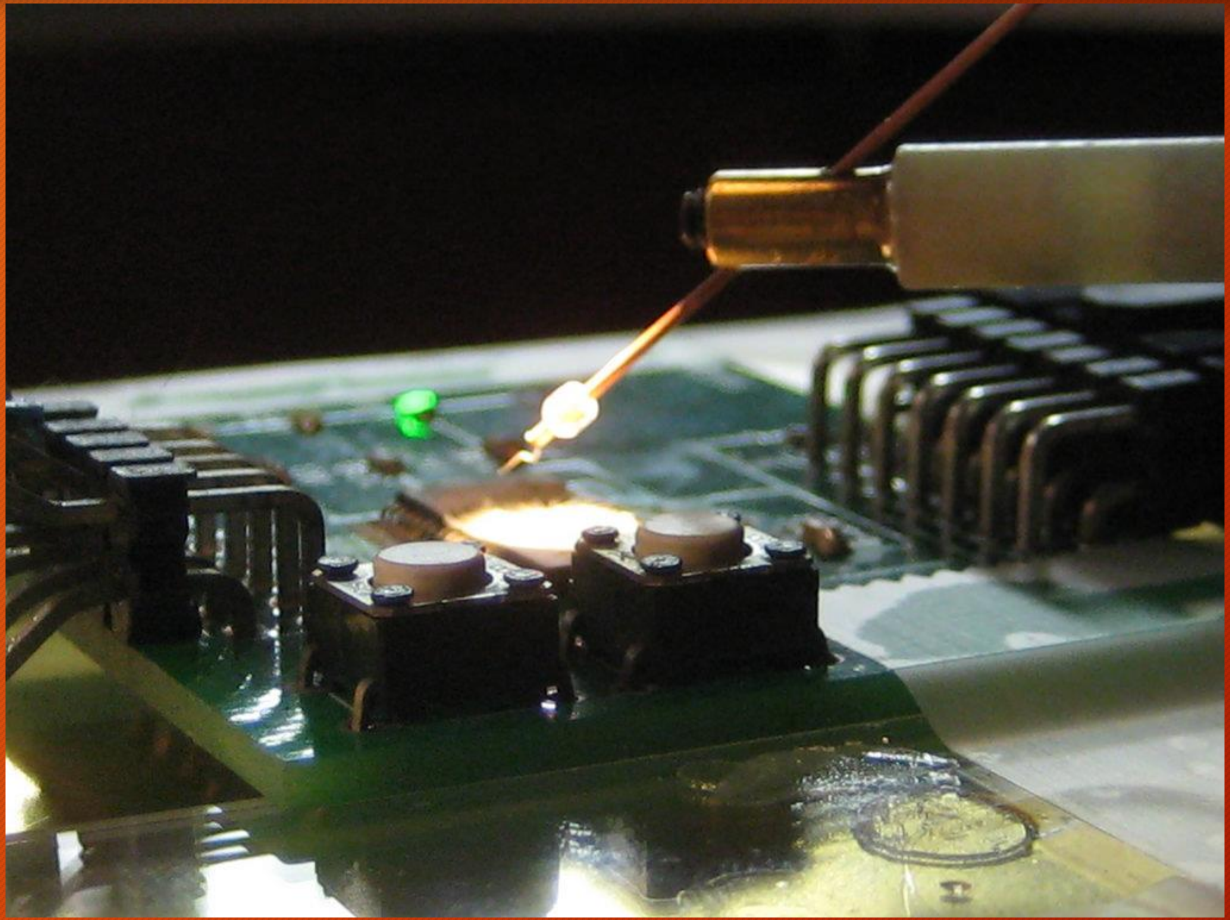


Image courtesy Travis Goodspeed – Read POC||GTFO for more goodness
https://www.flickr.com/photos/travisgoodspeed/3425845978/in/album-72157616476990240/

Microprobe key signals



https://www.flickr.com/photos/travisgoodspeed/3422351458/in/album-72157616476990240/

Reset protection fuses with UV

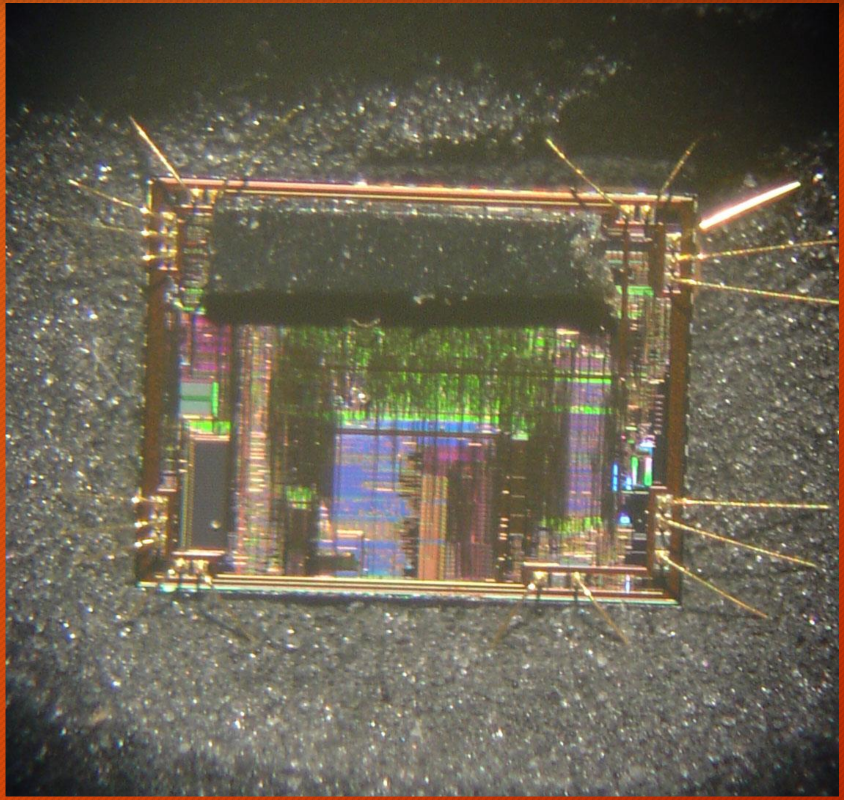


Image courtesy Bunnie Huang – google everything his does!
http://www.bunniestudios.com/blog/?page_id=40

Edit the chip using a Focused Ion Beam

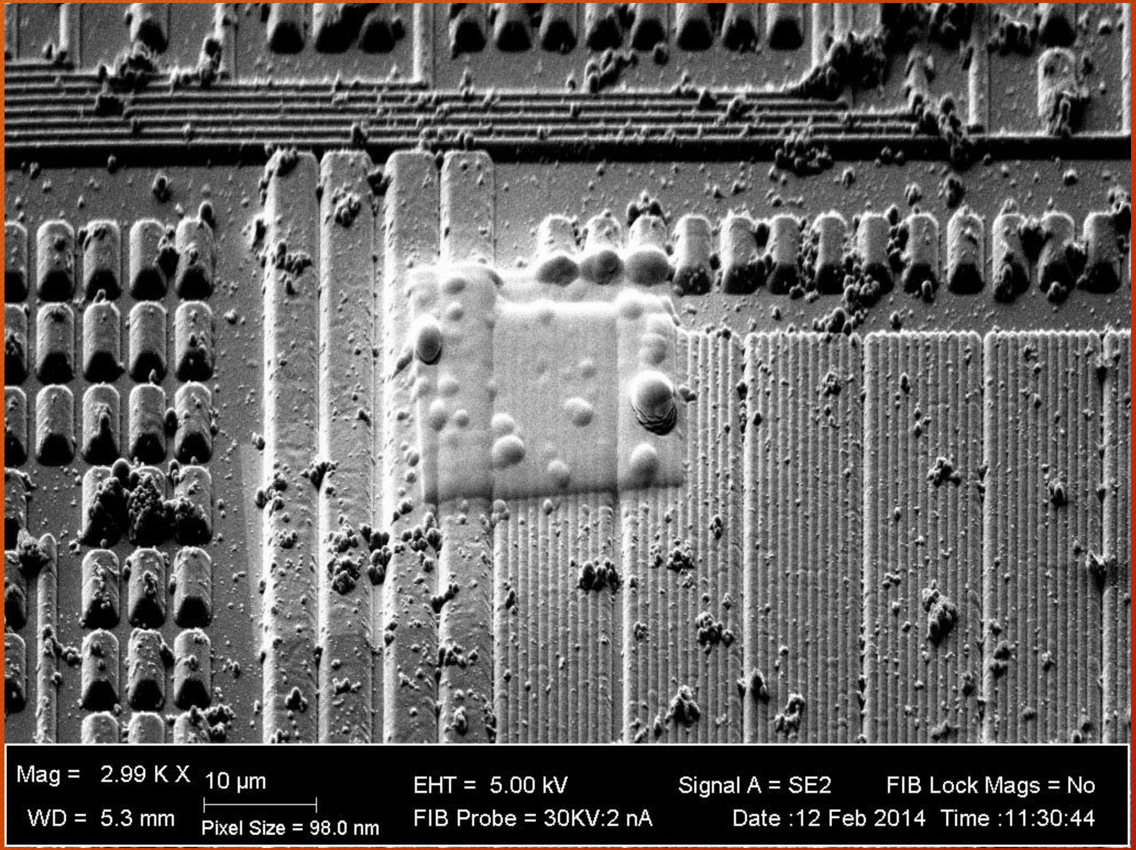
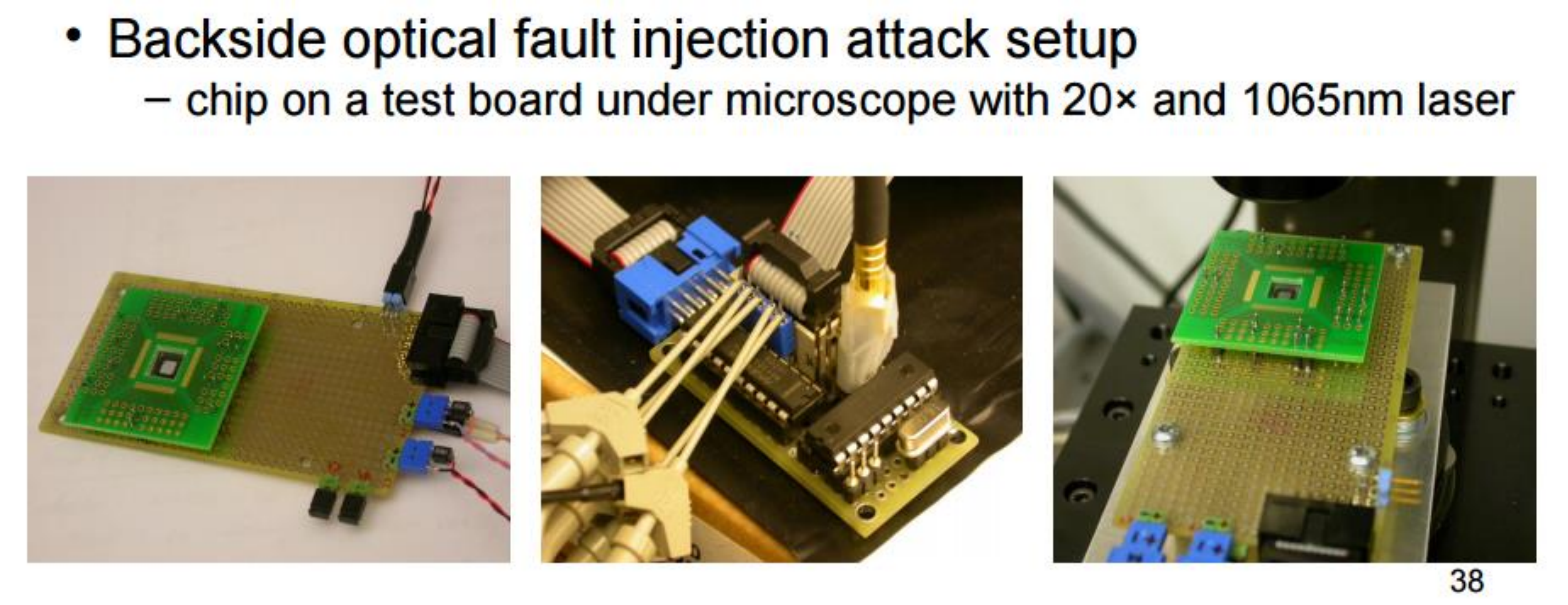


Image courtesy Andrew Zonenberg – who is way smarter then the presenter
http://siliconexposed.blogspot.com.au/2014/03/getting-my-feet-wet-with-invasive_31.html

Glitch areas of the chip using a laser



- Backside optical fault injection attack setup
  - chip on a test board under microscope with 20× and 1065nm laser

Image courtesy Dr Sergei Skorobogatov @ University of Cambridge England
https://www.cl.cam.ac.uk/~sps32/ECRYPT2011_1.pdf

So how do we protect chips

Integrate a metal layer mesh over critical areas

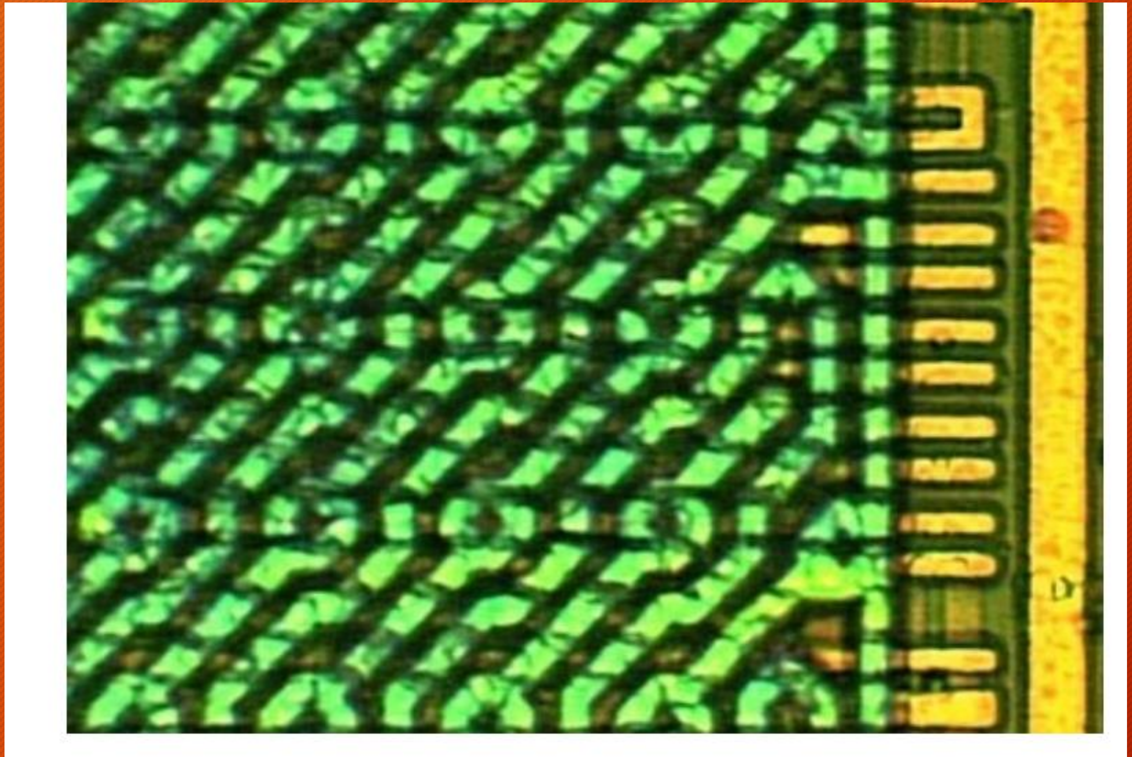


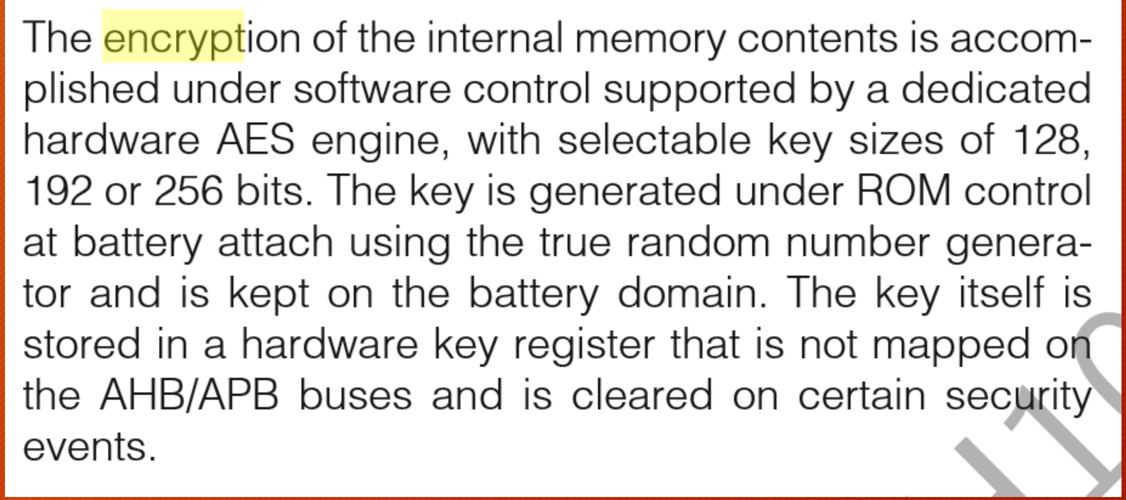
Image courtesy Oliver Kommerling
https://www.usenix.org/legacy/events/smartcard99/full_papers/kommerling/kommerling.pdf

Obfuscate the layout of critical areas of the chip

- Couldn’t find a good image ☹
- Just thing of a VLSI chip that looks like spaghetti
- Make it hard to automatically decode a chip area.

Scramble/Encrypt on-chip memories

- Helps protect memories from static memory dumping attacks
- However if you can probe the encryption engine you might be able to dump
- Helps – but is not a “Silver Bullet”



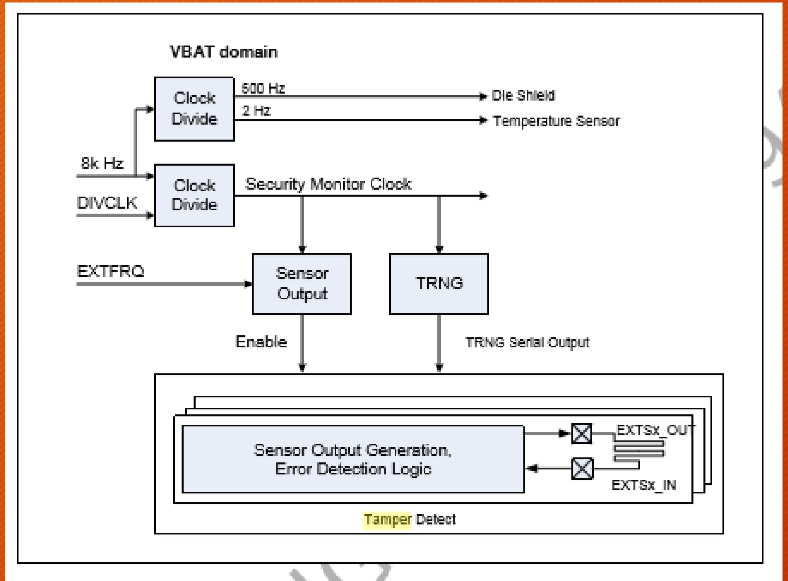
The encryption of the internal memory contents is accomplished under software control supported by a dedicated hardware AES engine, with selectable key sizes of 128, 192 or 256 bits. The key is generated under ROM control at battery attach using the true random number generator and is kept on the battery domain. The key itself is stored in a hardware key register that is not mapped on the AHB/APB buses and is cleared on certain security events.

Generate and roll unique crypto keys for each device.

- Attacks are physical in nature
- And take time
- And equipment
- And money
- So if you (securely) roll the crypto keys
- You’ll force the attacker to work quickly
- and they’ll only have a small time window to exploit
- And since keys are should be unique per device – they can’t take one “Master” key and break all your stuff.

Have active tamper detection mechanisms

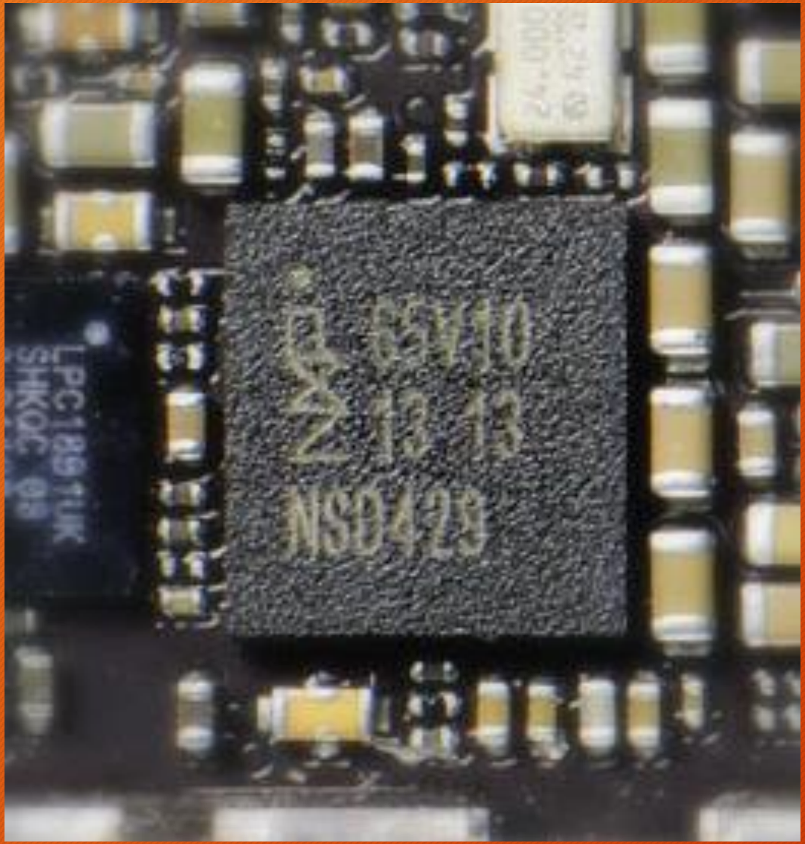
- Used in banking terminal – High Security Modules
- External meshes
- Cryptographic keys wiped if tamper detected
- Environmental protections
- Side channel protections.

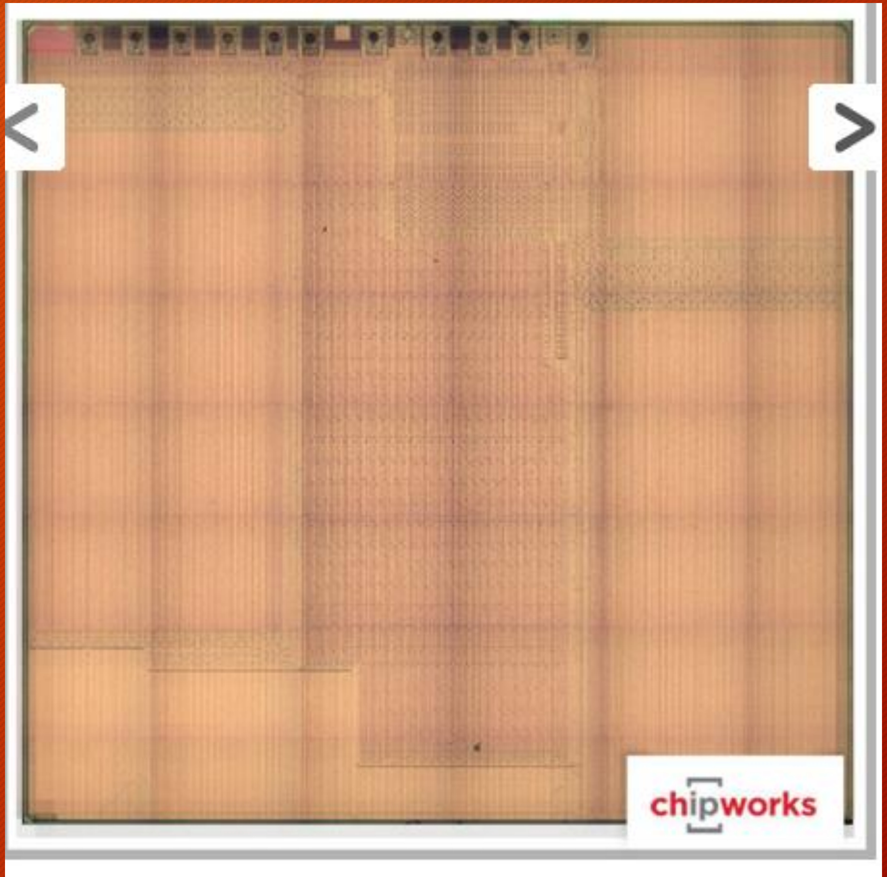


So the Fedz Vs Apple…

- Apple did a pretty good job considering threat model of 2+ years ago
- Unique keys per user/device! Not accessible in software mechanisms, Encrypted Memory!
- But memory wipe counter is stored in the flash
- So this can be “reset” by reflashing it with a good image.
- From iPhone 6 (A7 processor) they added a “Secure Enclave” block.
- Which is used to hold fingerprints and the counter.
- But physical attacks are also practical and feasible.

“Secure Element” for banking





NXP65V10 NFC controller and secure element

So iPhone 7

- Will probably add “Secure Element” style protections on the die.
- And active tamper responses to deter attack
- And a pony

Wrapping Up.

- Physical attacks are pretty cool
- And feasible given time and equipment
- But can be mitigated!
- Break stuff and look at it.
- Just don’t breathe the acid it in.
- Or touch it – well room temp. 70% nitric is fine (just makes your skin turn yellow for a little bit)
- Read and watch http://www.murdochspirates.com/

People I stole stuff from/references

- Andrew Zonenberg - http://siliconexposed.blogspot.com.au/
- Dmitry Nedospasov - http://www.nedos.net/about/
- Oliver Thomas - http://www.texplained.com/
- Oliver Kömmerling/Markus Kuhn
- Dr Sergei Skorobogatov - http://www.cl.cam.ac.uk/~sps32/
- Bunnie Huang - http://www.bunniestudios.com/
- Travis “Good Neighbour” Goodspeed – http://travisgoodspeed.blogspot.com.au/
- John McMaster - http://uvicrec.blogspot.com.au/

And all the other I missed ☹

Definitely a Con's

https://wrongisland.org/

http://unrestcon.org/