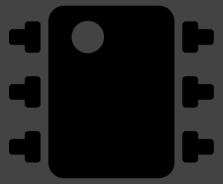
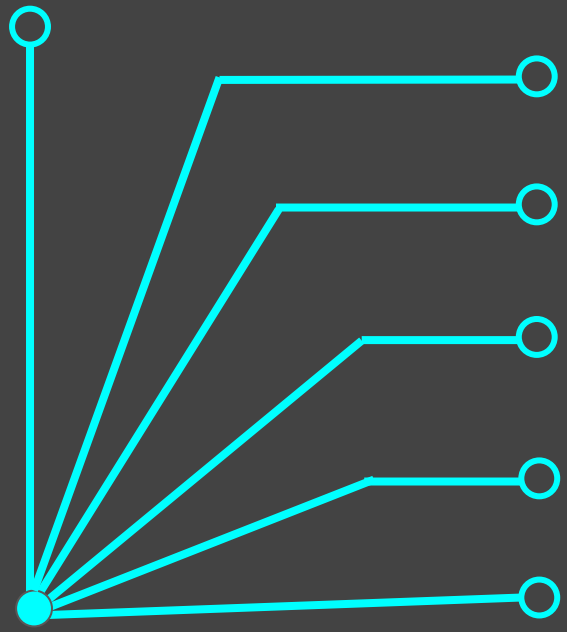
Engenharia reversa *in Silico*

Desmistificando o Silício

https://tinyurl.com/revsilico



$ whoami



Bruno Rafael Aricó

Graduado em Ciência da Computação (IME-USP)

Especialização em sistemas embarcados (Cin-UFPE)

Cofundador do grupo Hardware Livre USP

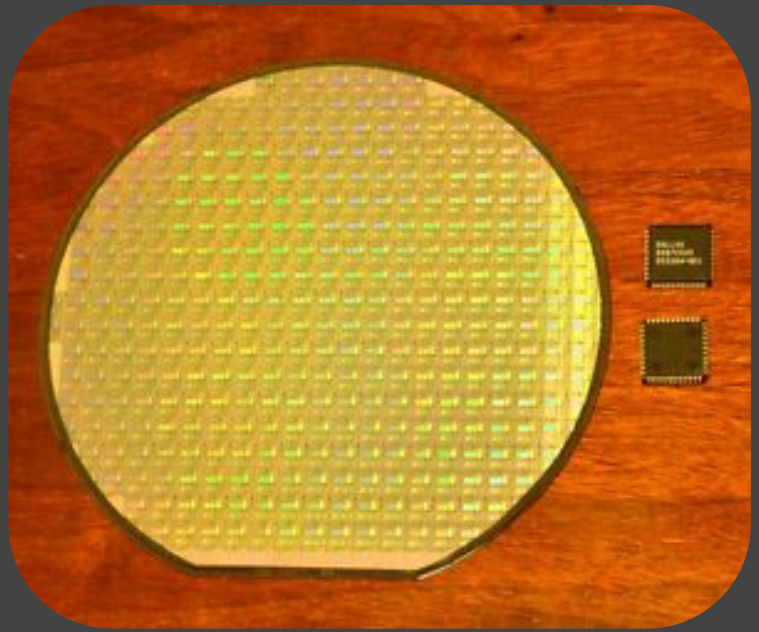
Prototipagem rápida

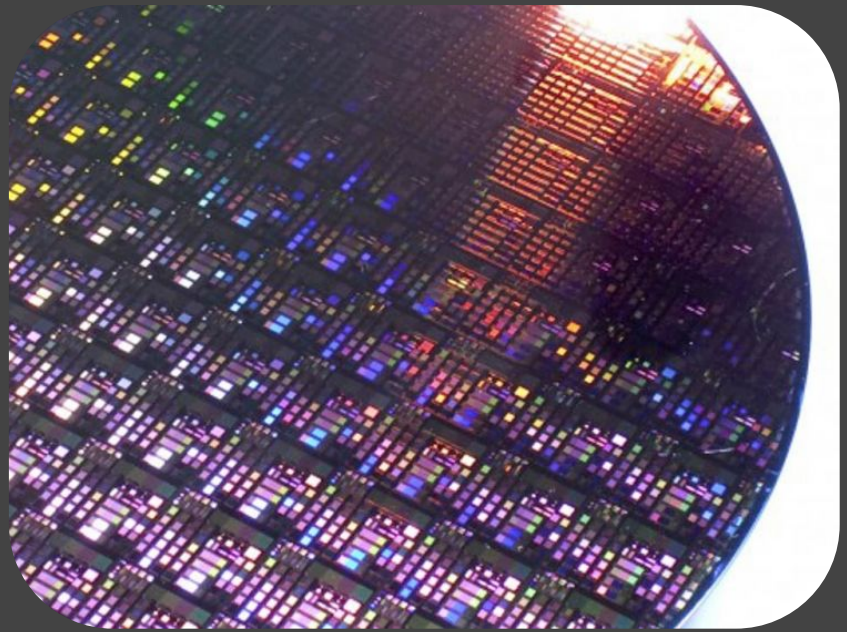
E-mail: brunoarico@gmail.com Site: www.linux.ime.usp.br/~brunobra

$ ls

1. Motivação
2. Contextualização do problema
3. Como funcionam os semicondutores
4. Apresentação da técnica/resultados
5. Aplicação
6. Easter Eggs

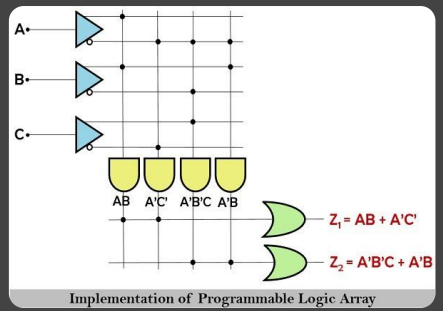
$ O Silicio



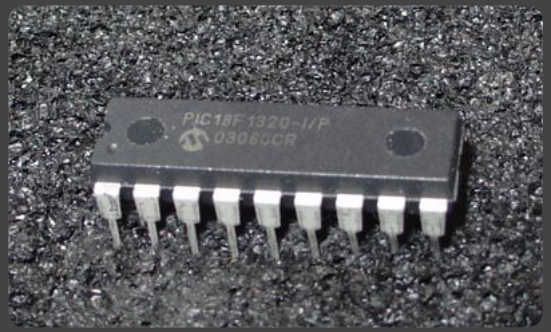


$ Por que explorar o silício?

- Entender falhas a fundo



- Extrair informaçoes de firmware



$ Por que explorar o silício?

- Cybersecurity

Notícias > Antivírus e Segurança

É com este chip que a China teria se infiltrado na Apple, Amazon e outras empresas americanas

Placas mãe para servidores da Supermicro teriam chip do tamanho de um grão de arroz para espionar gigantes dos Estados Unidos

How sure are you the ESP32 is not a Trojan horse?

General

No other vendor offers a part so well featured and inexpensive for massive network deployment. Which makes me wonder, maybe it is too good to be true? What if the totalitarian government designed in a switch that has never been used yet?

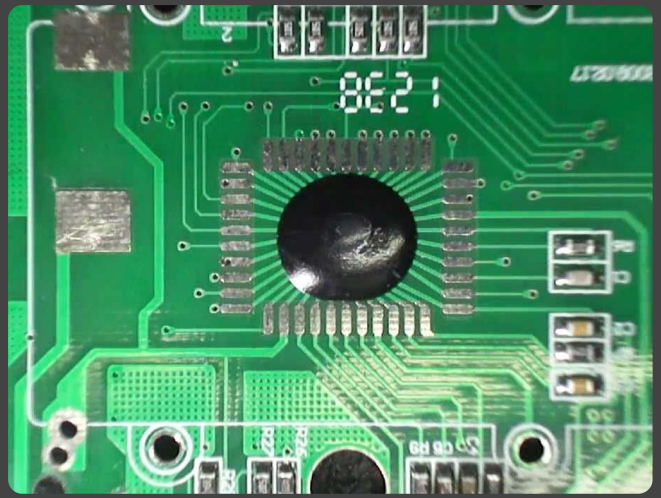
I know this could be true in any tech, and from many countries, but I single this one out because the cost and impact ratio seems to be the best for potential abuse.

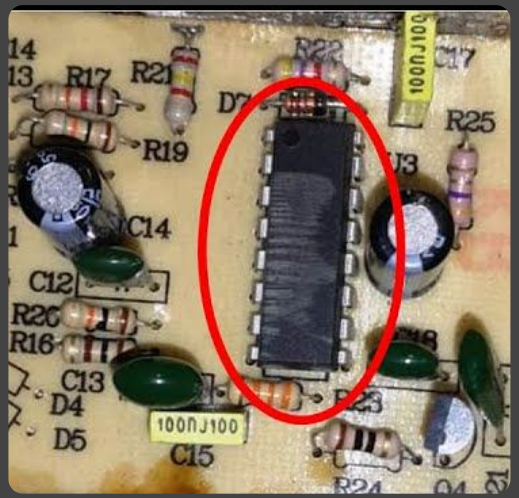
What are the risks and mitigations? Are potential users considering this when they select it, or rule it out?

?

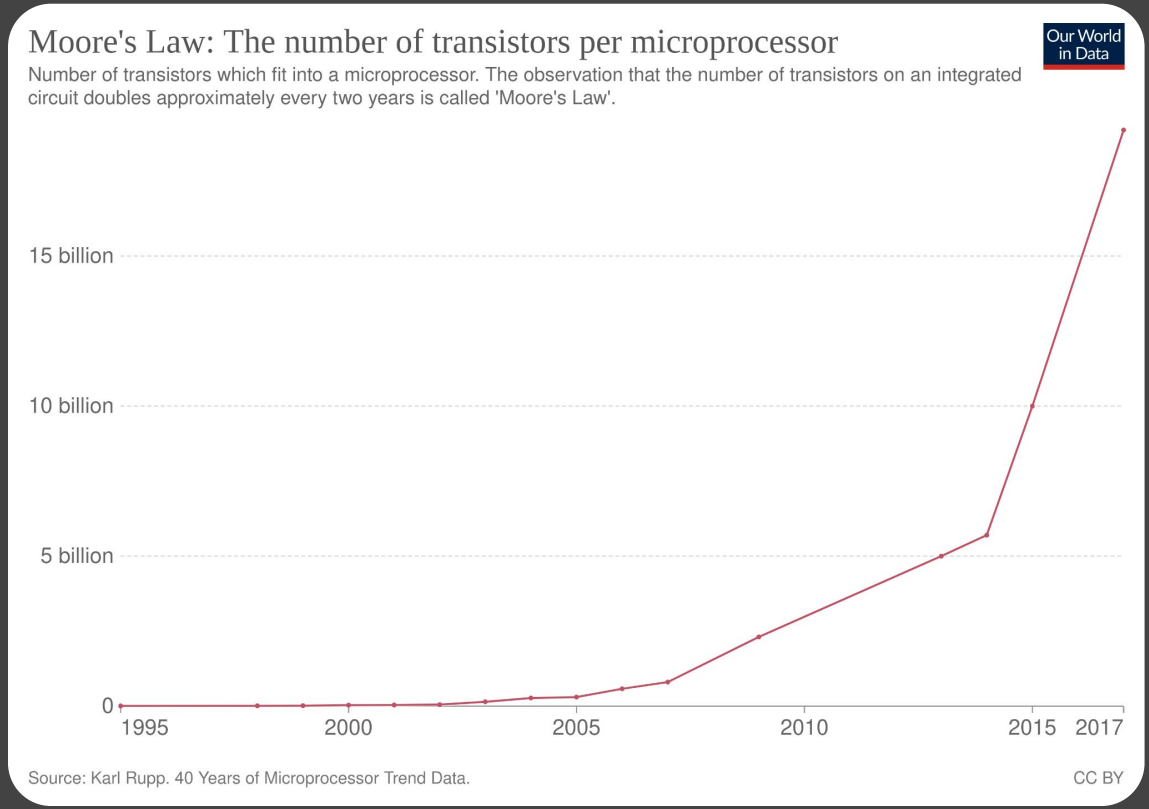
$ Por que explorar o silício?

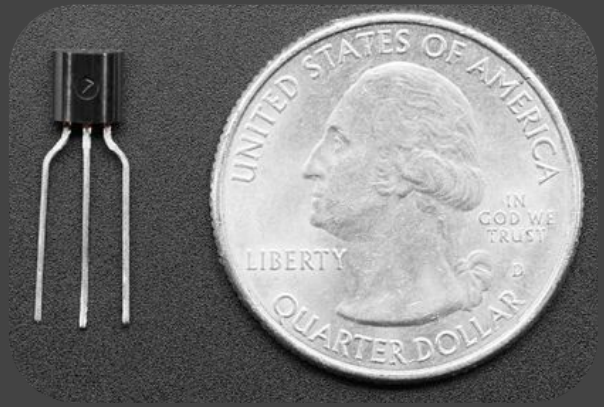
- Entender funcionalidade de CI’s

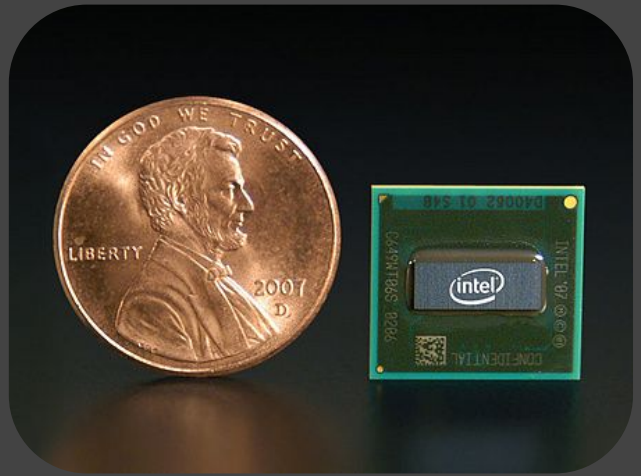




$ Transistores





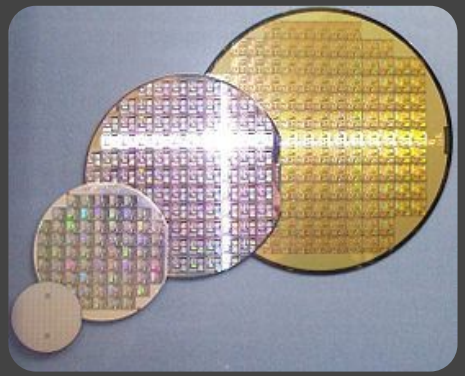


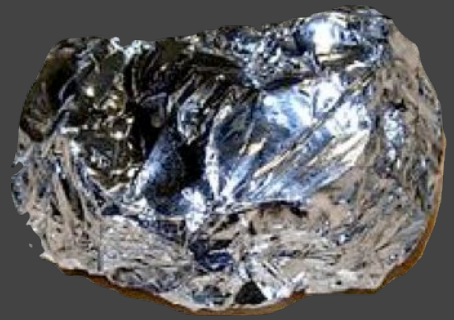
$ Quão pequeno é um transistor hoje?

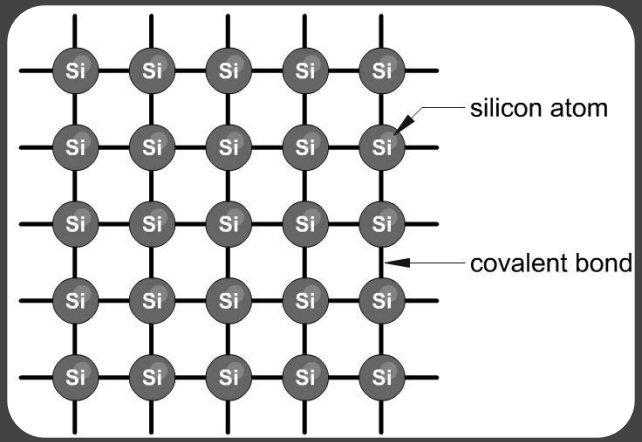



	I9 13900k	I9 9900k	Core 2 DUO	i486	Z-80
Tecnologia	7nm	14 nm	45-65 nm	800 nm	4000 nm
Ano	2023	2018	2006	1991	1976
Transistores	26 bi	7 bi	290 mi	1.6 mi	8500

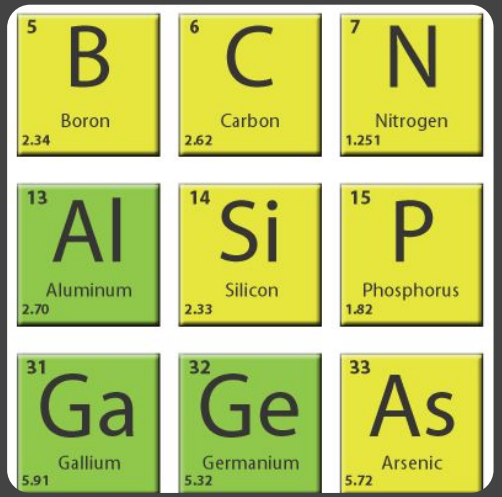
$ O silício



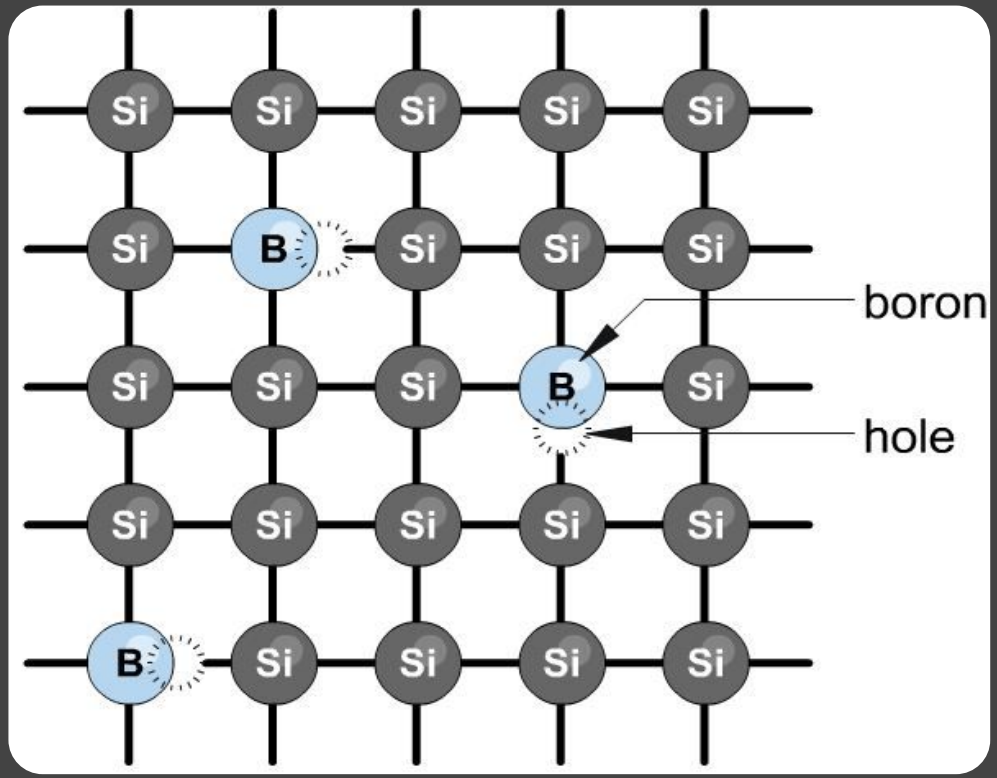


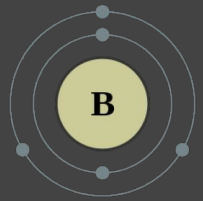


O silício não conduz bem elétrons à temperatura ambiente

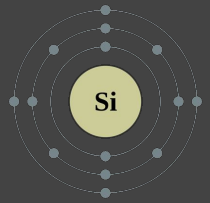


$ Tornando o silício condutor





3 elétrons de valência

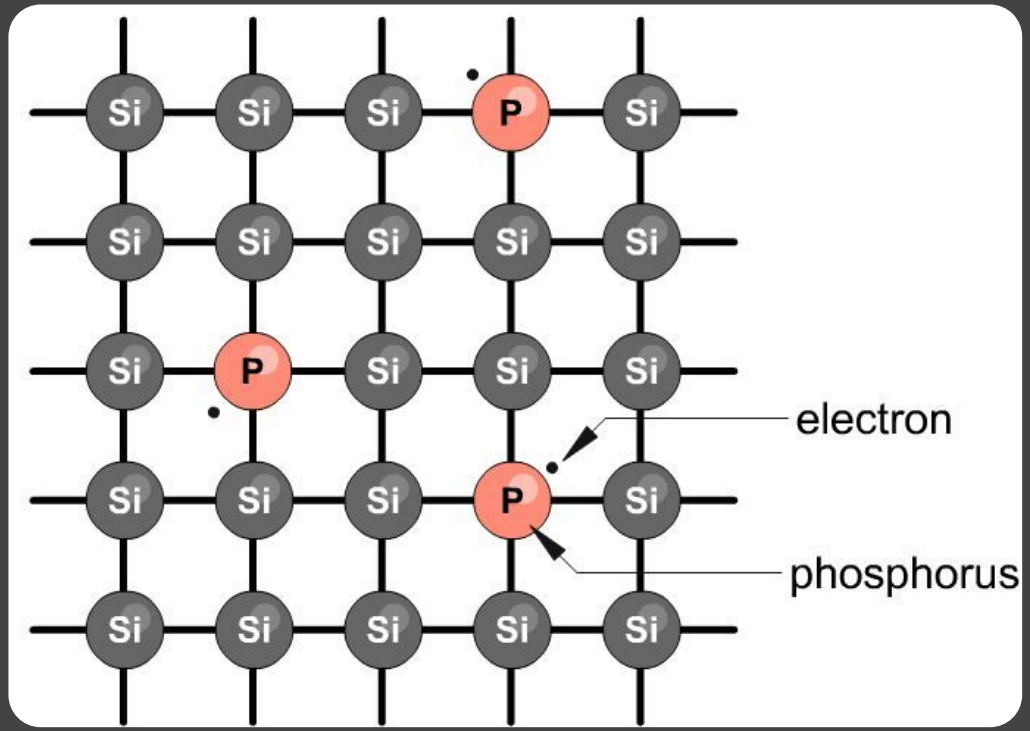


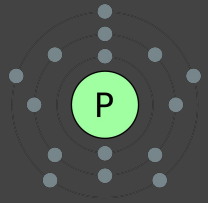
4 elétrons de valência

Os **buracos** são ausência de elétrons, interpretados como cargas positivas

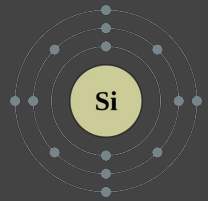
Esse é um silício com dopagem **tipo P** (Positiva)

$ Tornando o silício condutor





4 elétrons de valência

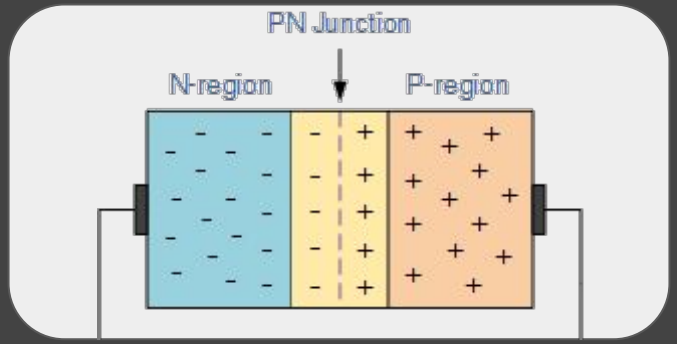


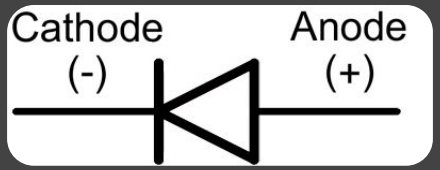
4 elétrons de valência

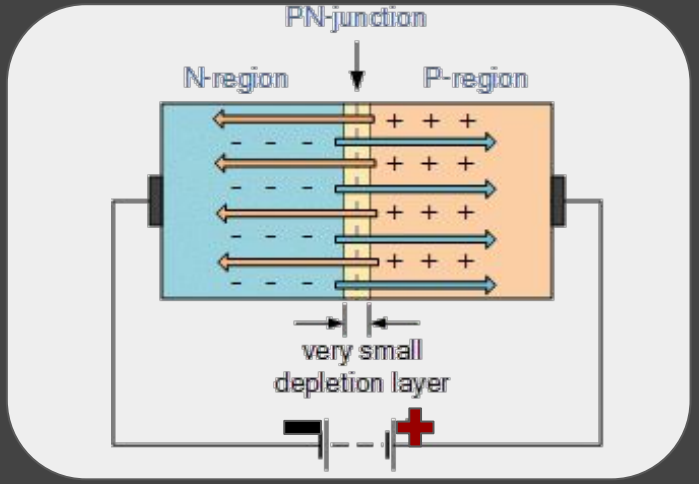
Como o Fósforo tem 5 elétrons de valência, um deles fica livre no reticulado, conferindo uma carga **negativa**.

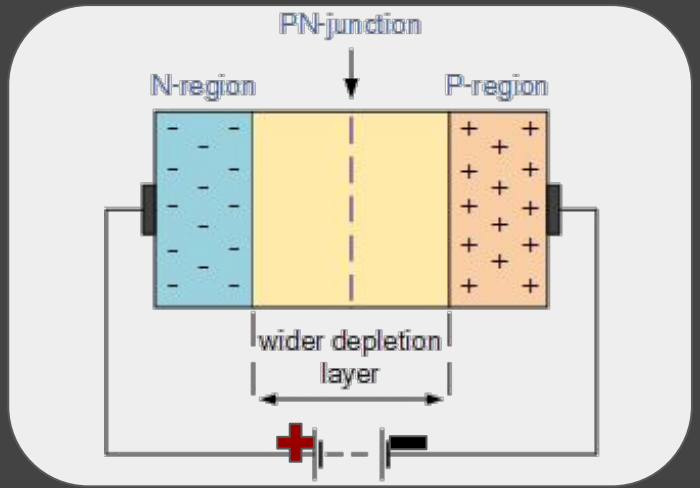
Esse é um silício com dopagem **tipo N** (Negativa)

$ O diodo


PN Junction
N-region
P-region

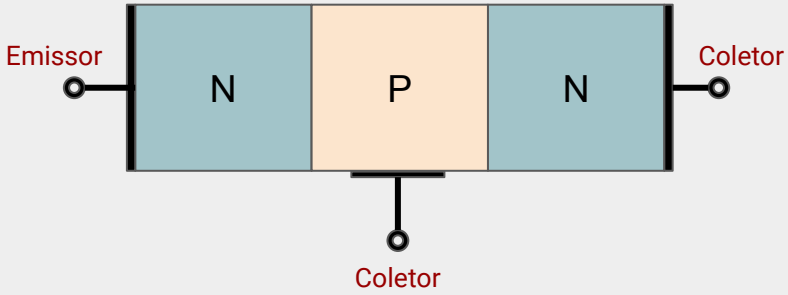

Cathode
(-)
Anode
(+)


PN-junction
N-region
P-region
very small
depletion layer

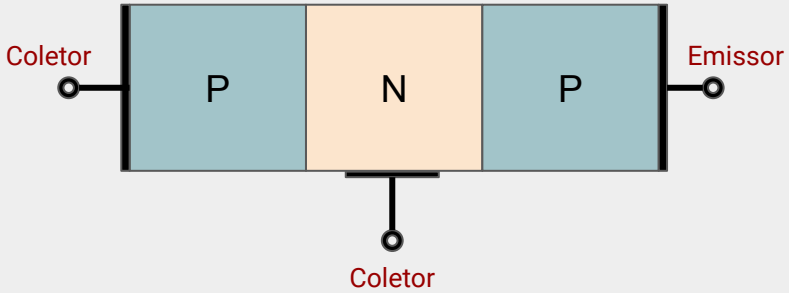

PN-junction
N-region
P-region
wider depletion
layer

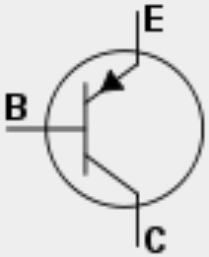
$ O transistor

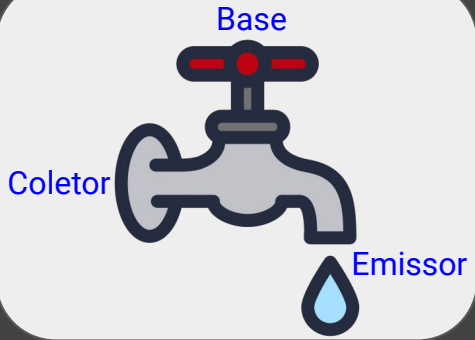
Transistor NPN

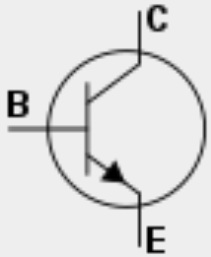


Transistor PNP

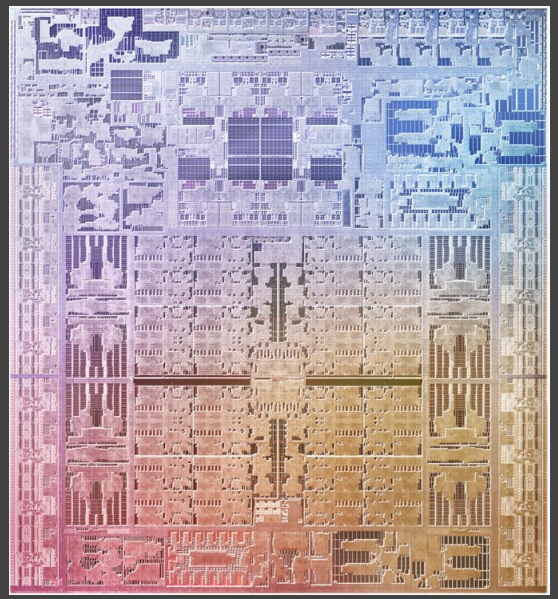


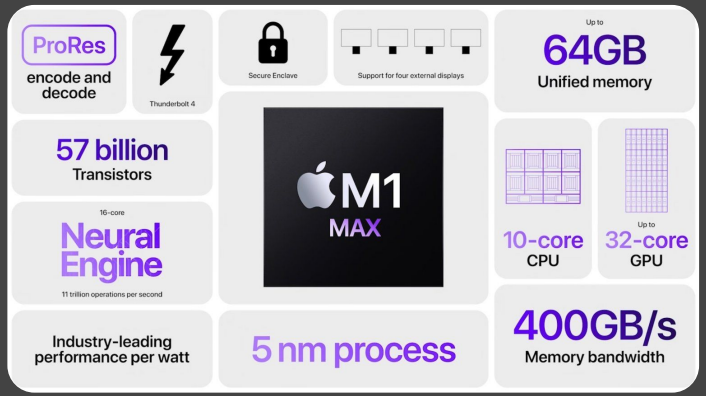




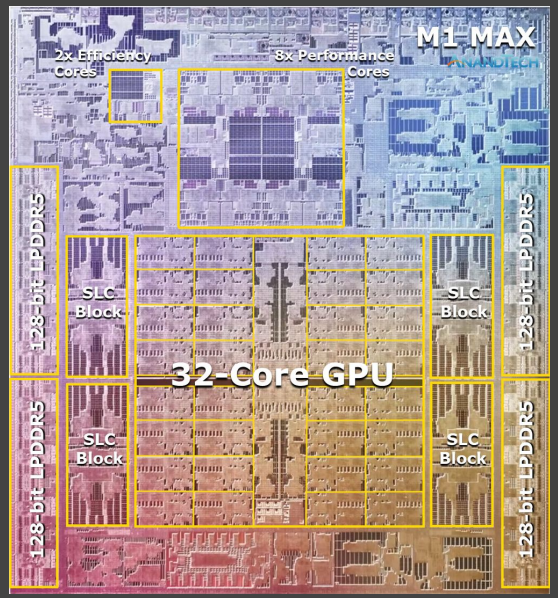


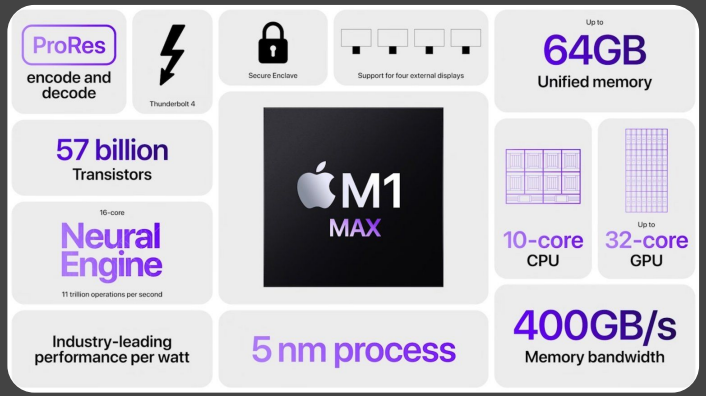
$ Quão pequeno é um transistor hoje?



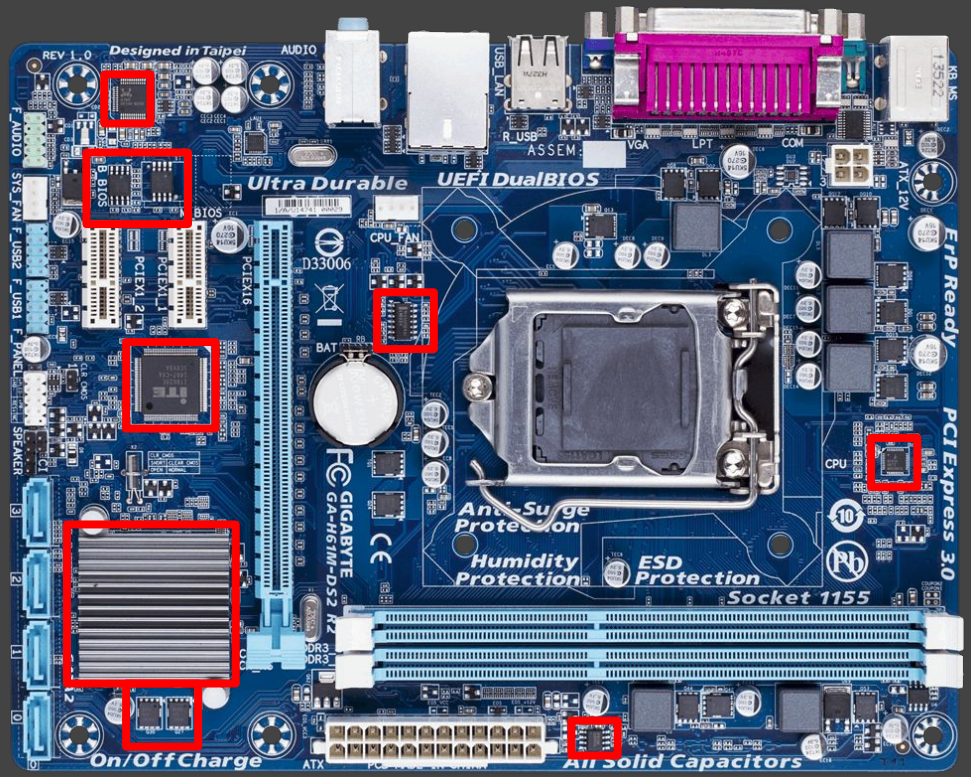


$ Quão pequeno é um transistor hoje?

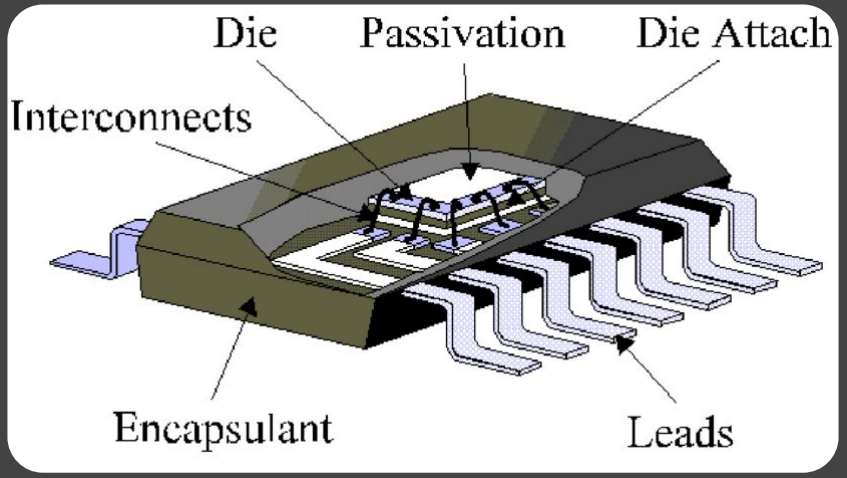


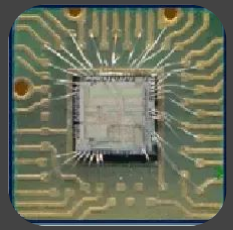


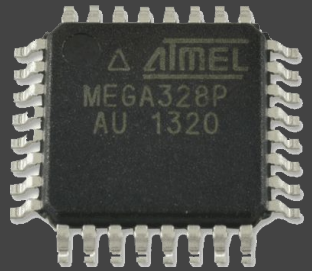
$ Nem tudo é tão miniaturizado!



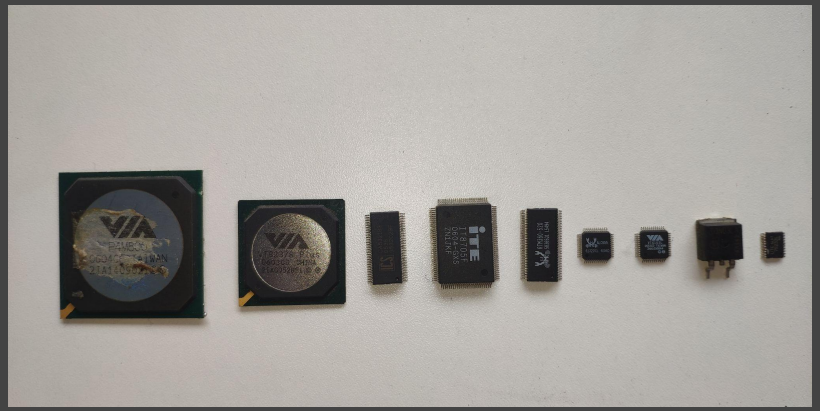
$ Onde está o silício?

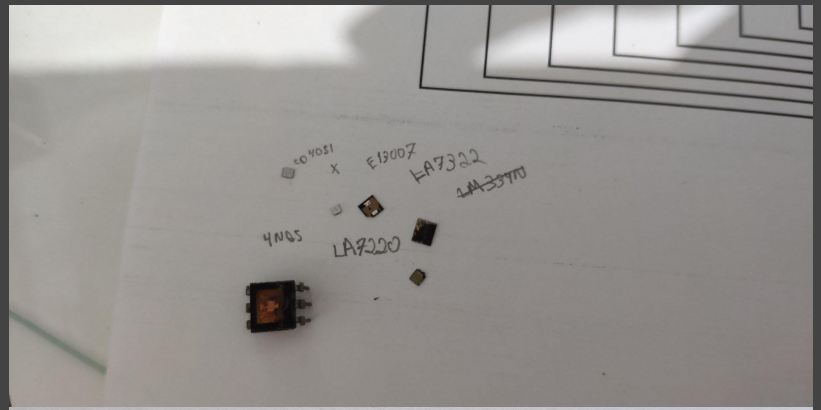


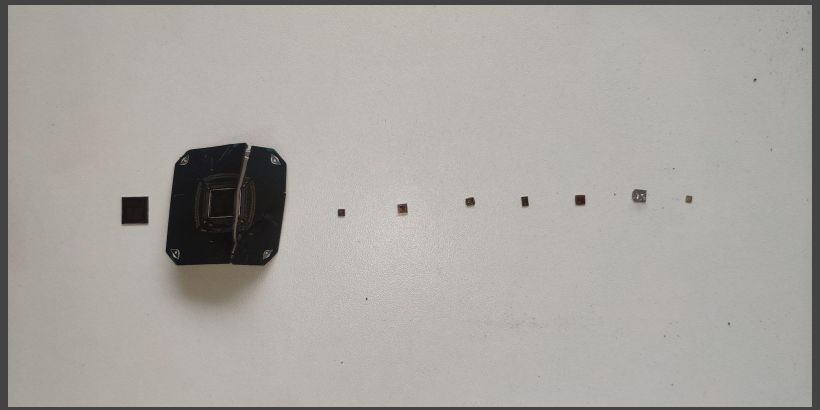


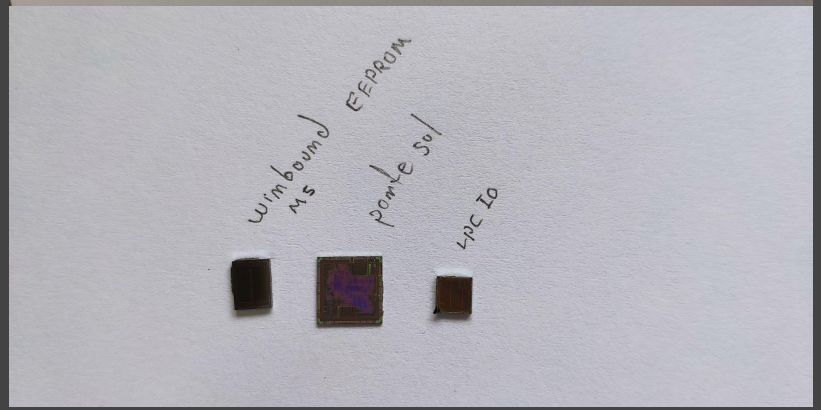


$ Onde está o silício?









$ Tecnicas de decapsulamento

- Extração com abrasão
- Extração com ácido
- Extração com soprador térmico
- Extração com ácido e soprador térmico
- Extração com resina de colofonia

Mais técnicas e mais detalhes em:
https://siliconpr0n.org/

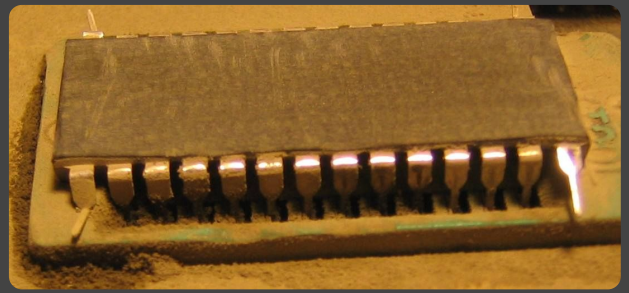
$ Extração com por abrasão

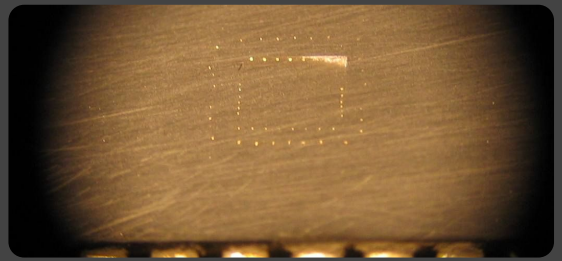
Procedimento 1:

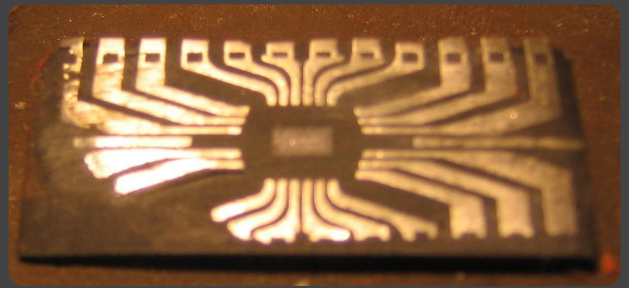
- Lixar com lixas cada de grão elevado (100)
- Ao perceber mudanças de padrão na superfície, diminuir o grão progressivamente

Caso você tenha um potente

10/10

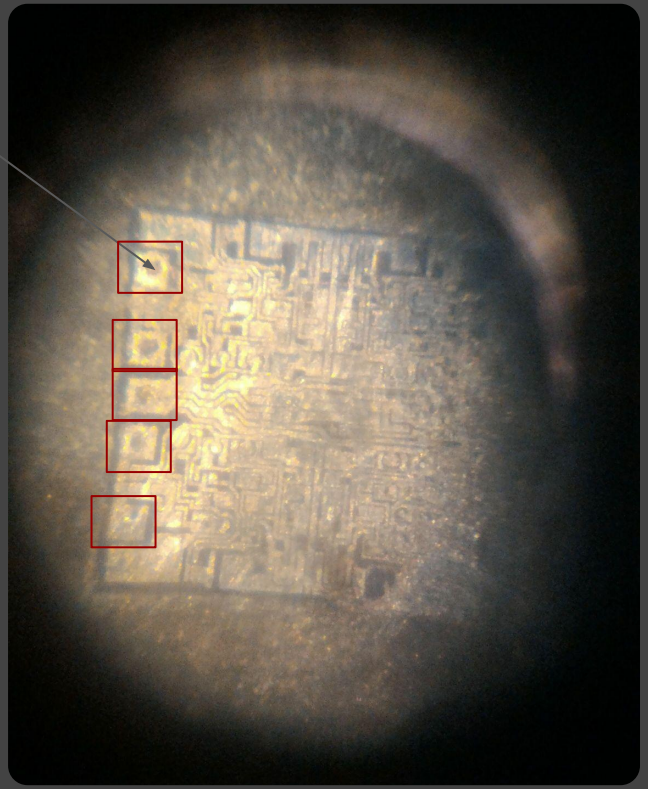


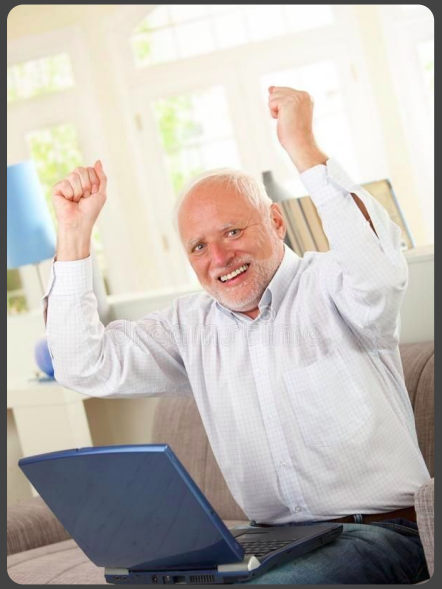




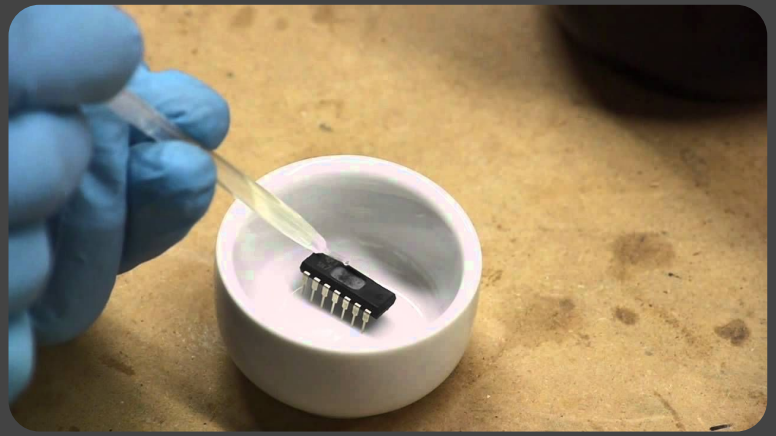
$ Resultado

pads





$ Extração a quente com HNO_3



t4f

BLOG | PROJECTS | ARTICLES | SHOP | ABOUT ME

Tech For Fun

POSTED ON TUESDAY FEBRUARY 4TH, 2014 BY RAMIRO

ultra-low cost ic decapsulation

or how to decap microcontrollers at home and cut your life expectancy in 20 years

ARCHIVES

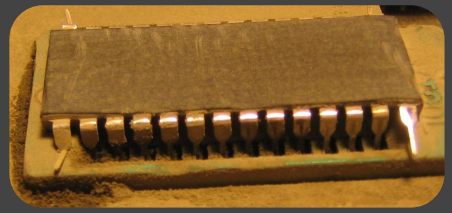
Archives

Select Month

$ Extração a quente com HNO_3

Procedimento:

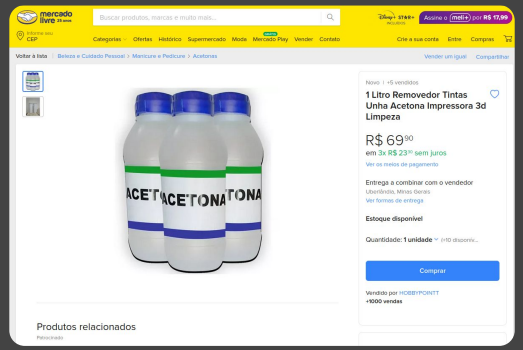
- (A ser testado: deixar o CI de molho em etileno glicol)
- Desbastar o epoxi cuidadosamente
- Imergir o chip em ácido nítrico (conc >60%)
- Aquecimento em banho maria (Até diluir o epoxy)
- Filtragem
- Lavagem com água
- Lavagem com acetona concentrada
- Lavagem com isopropanol

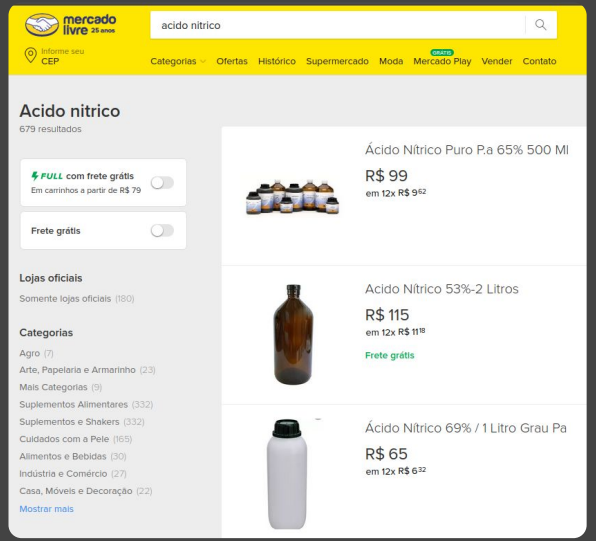


$ Extração a quente com HNO_3

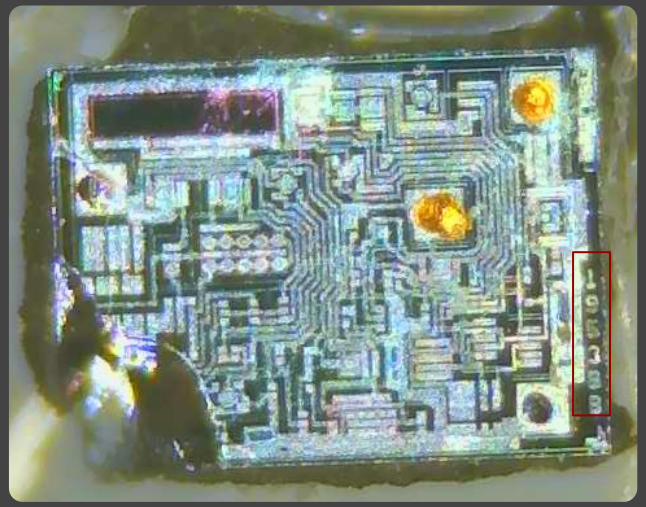
Procedimento:

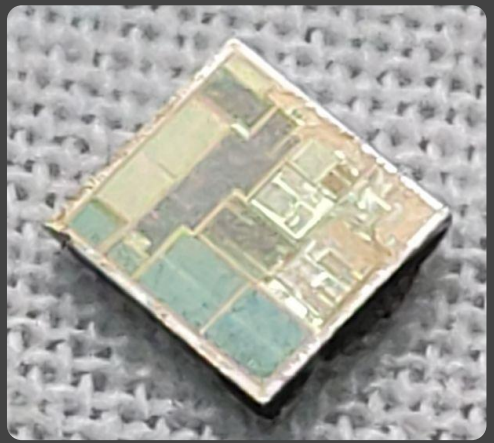
- (A ser testado: deixar o CI de molho em etileno glicol)
- Desbastar o epoxi cuidadosamente
- Imergir o chip em ácido nítrico (conc >60%)
- Aquecimento em banho maria (Até diluir o epoxy)
- Filtragem
- Lavagem com água
- Lavagem com acetona concentrada
- Lavagem com isopropanol





$ Resultado





$ Extração com Soprador térmico

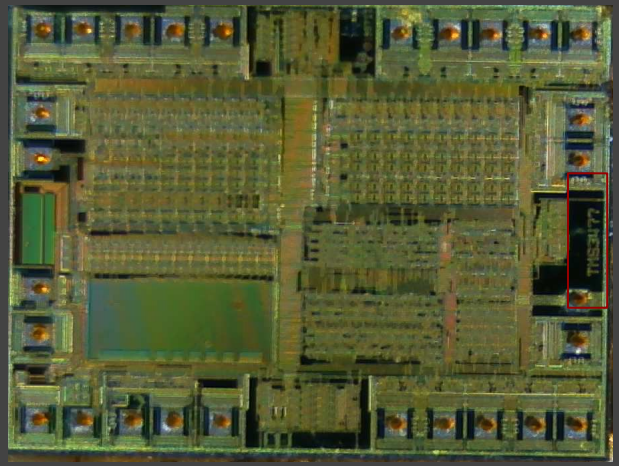
Procedimento:

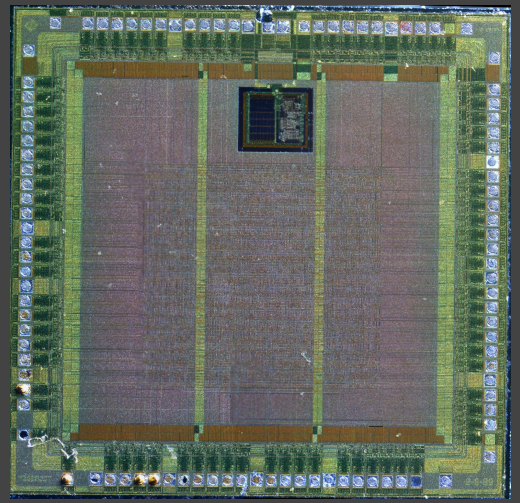
- Prender o chip em uma morsa
- Ajustar o soprador termico para 450C
- Ajustar o fluxo de ar para o maximo
- Jogar ar sobre o chip por 1 min
- Cuidadosamente ir removendo o epoxi até chegar no silício

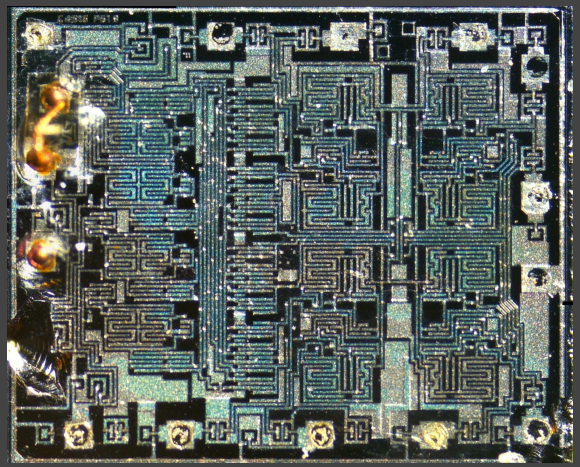
$ Resultado


TMS3477NL
MTW 323
02385 PHILIPPINES

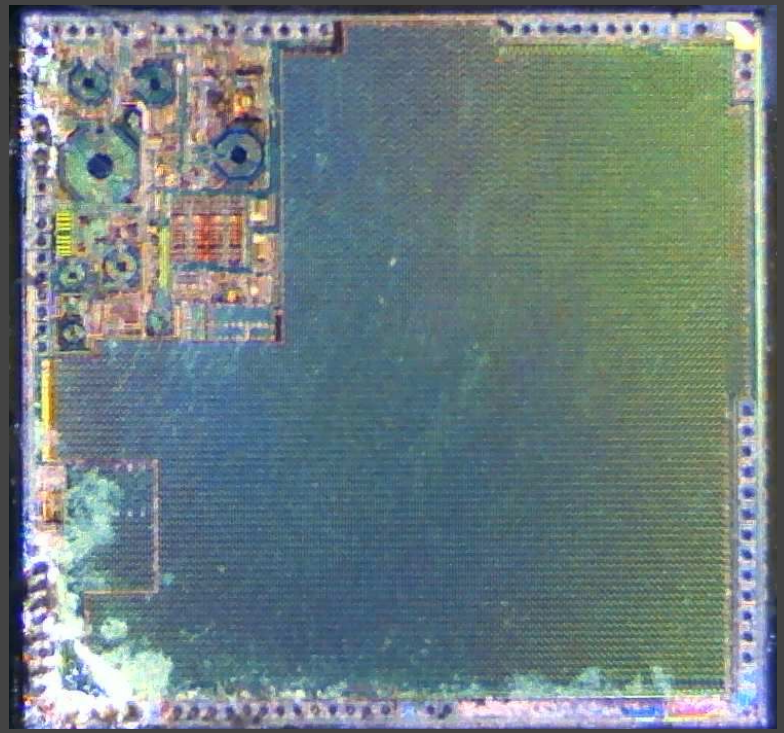

TESTED
TESTED
TESTED
7/10

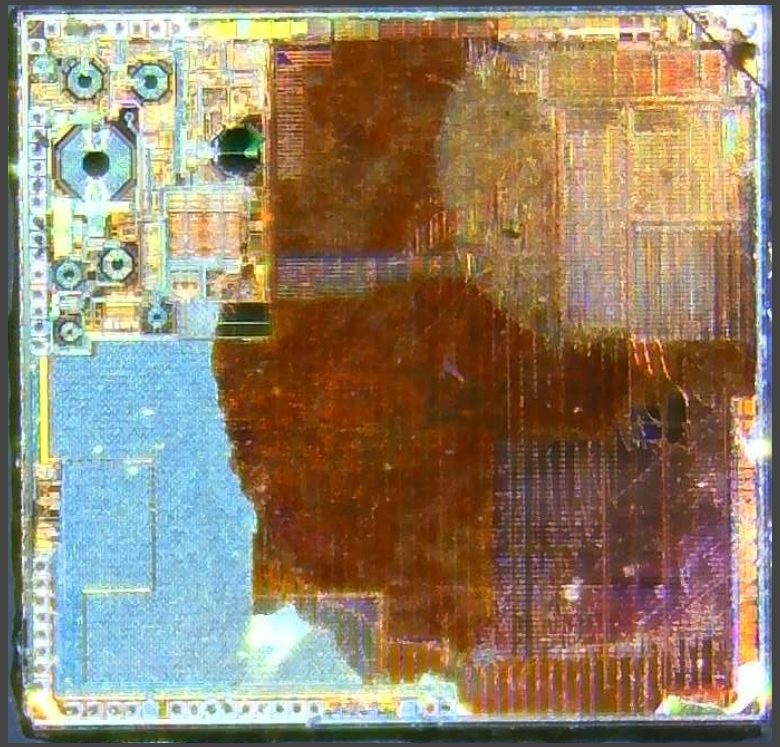




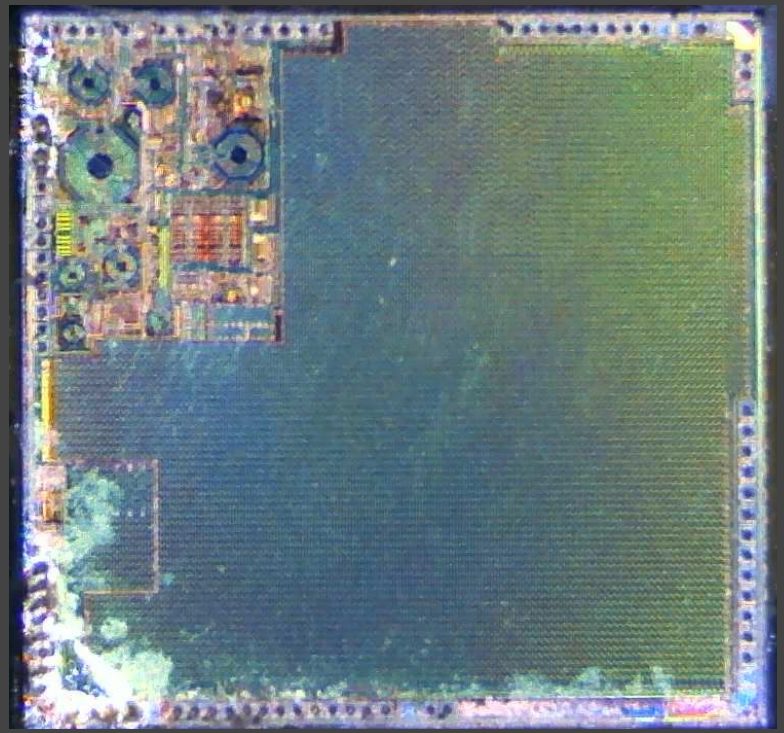


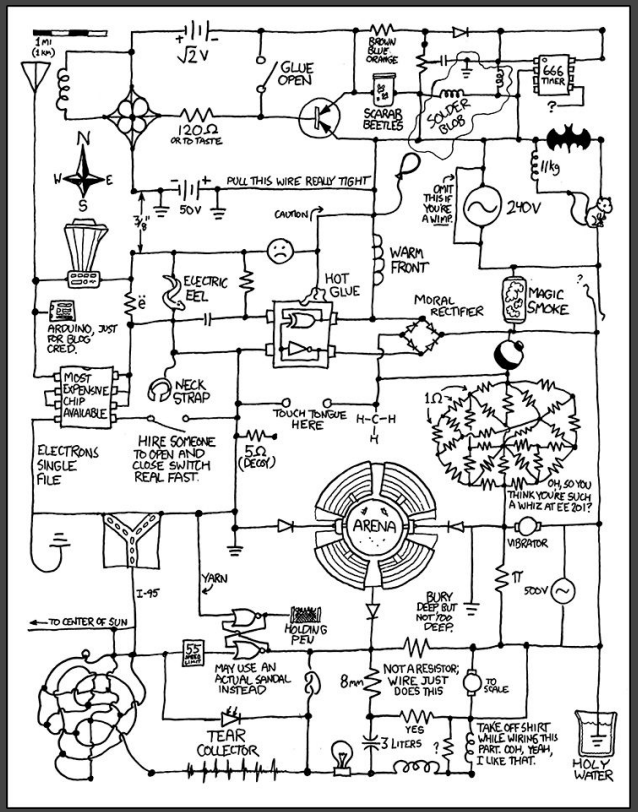
$ Resultado



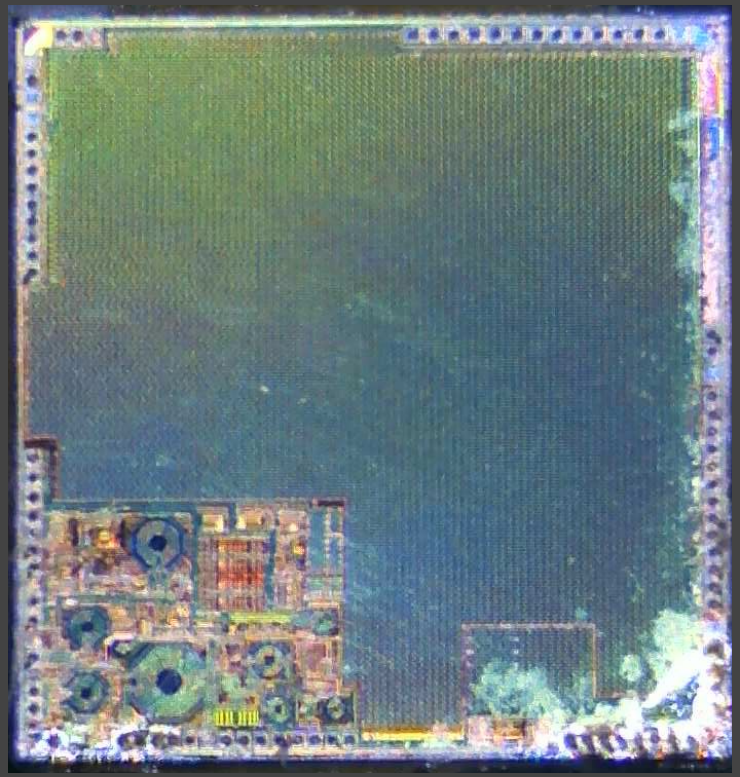


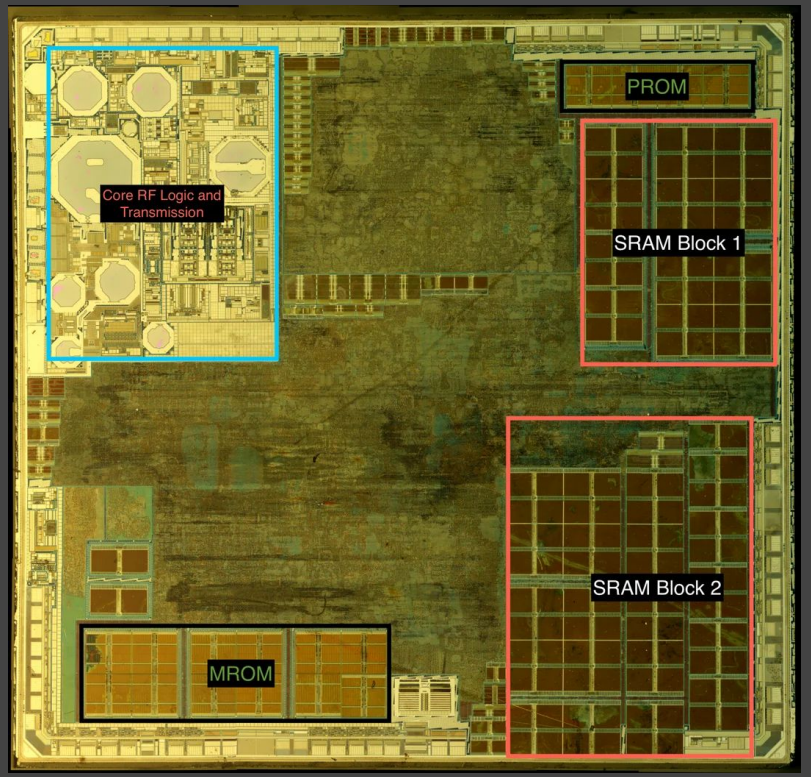
$ Resultado




√2V
GLUE OPEN
120Ω OR TO TASTE
SCARAB BEETLES
SOLDER BLOB
666 TIMER
PULL THIS WIRE REALLY TIGHT
50V
CAUTION
240V
WARM FRONT
ELECTRIC EEL
HOT GLUE
MORAL RECTIFIER
MAGIC SMOKE
ARDUINO, JUST FOR BLOG CRED.
MOST EXPENSIVE CHIP AVAILABLE
NECK STRAP
TOUCH TONGUE HERE
H-C-H
ELECTRONS SINGLE FILE
HIRE SOMEONE TO OPEN AND CLOSE SWITCH REAL FAST.
5Ω (DECOY)
OH, SO YOU THINK YOU'RE SUCH A WHIZ AT EE 201?
ARENA
VIBRATOR
I-95
YARN
BURY DEEP BUT NOT TOO DEEP.
TO CENTER OF SUN
HOLDING PEN
MAY USE AN ACTUAL SANDAL INSTEAD
NOT A RESISTOR; WIRE JUST DOES THIS
TO SCALE
TEAR COLLECTOR
3 LITERS
YES
TAKE OFF SHIRT WHILE WIRING THIS PART. OOH, YEAH, I LIKE THAT.
HOLY WATER

$ Resultado



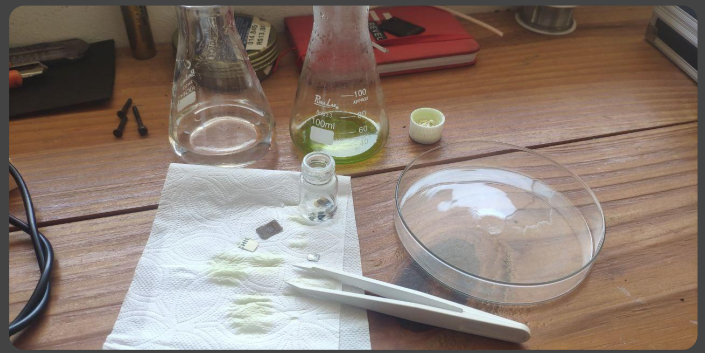

Core RF Logic and Transmission
PROM
SRAM Block 1
SRAM Block 2
MROM

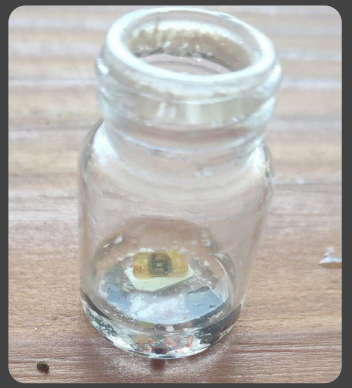
$ Extração a frio com HNO_3 e soprador

8/10

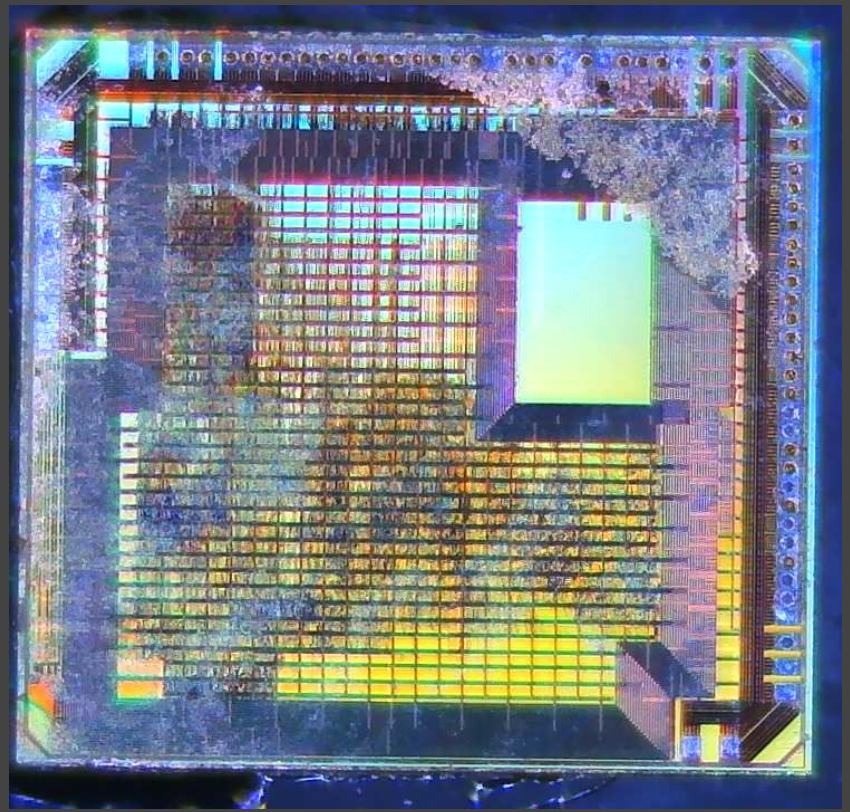
Procedimento 1:

- (A ser testado: deixar o CI de molho em etileno glicol)
- Imergir o chip em ácido nítrico (conc >60%)
- Deixar repousar por 1 semana no sol
- Filtragem
- Lavagem com água
- Lavagem com isopropanol
- Extração com o método do soprador térmico

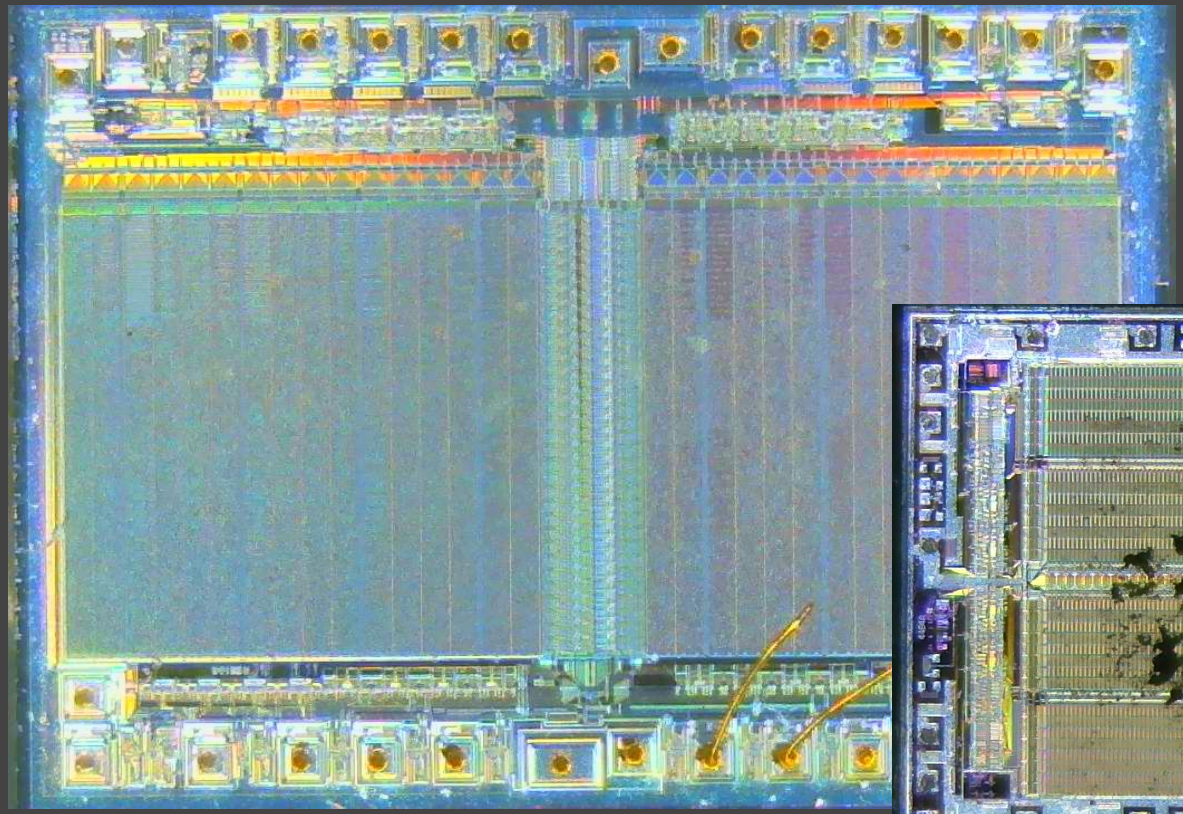


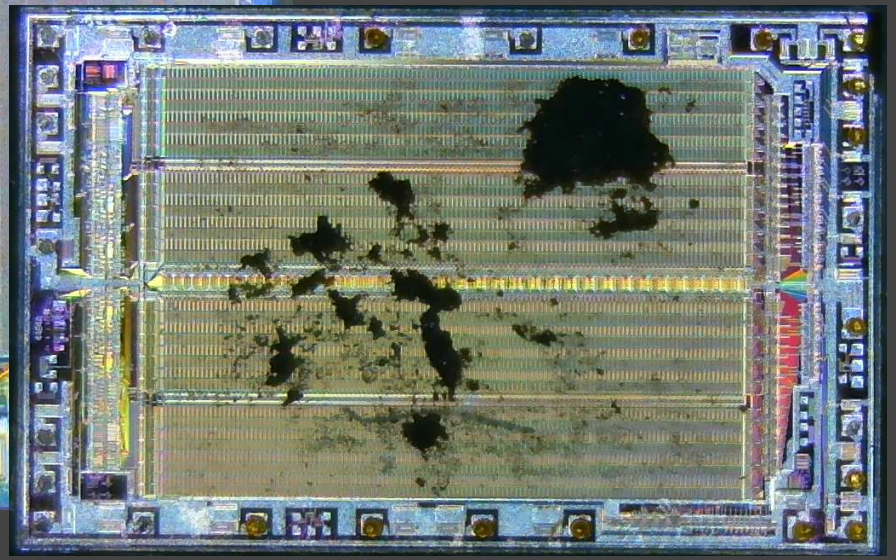


$ Resultado



$ Resultado

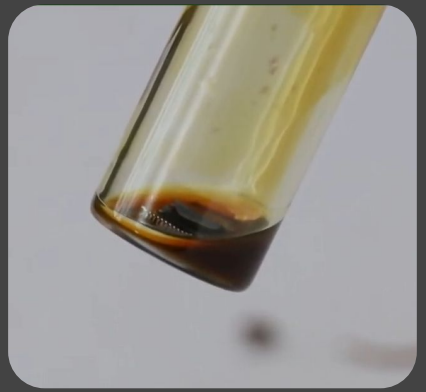




$ Extração com breu (Colofonia)

Procedimento:

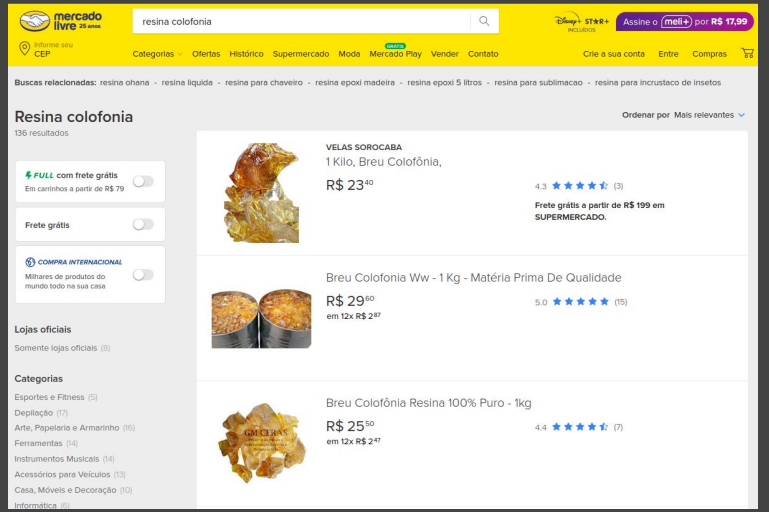
- Desbastar o epoxi cuidadosamente
- Imergir o chip em resina de colofonia aquecida (450C)
- Aquecimento em banho maria (Até diluir o epoxy)
- Filtragem
- Lavagem com água
- Lavagem com acetona concentrada
- Lavagem com isopropanol



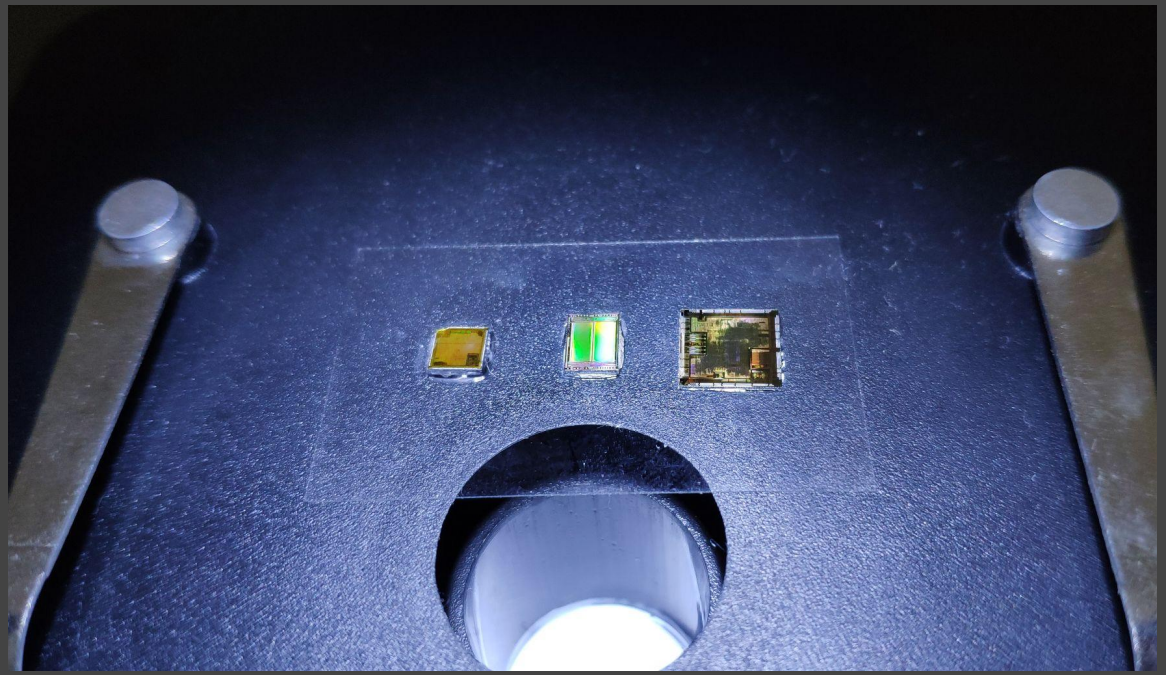
$ Extração com breu (Colofonia)

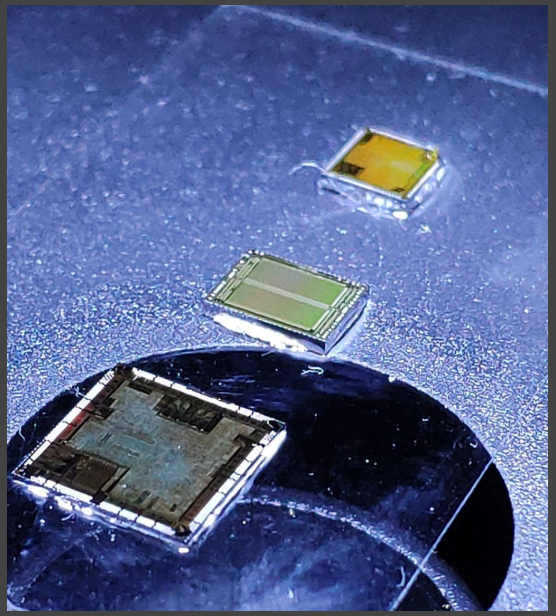
Procedimento:

- Desbastar o epoxi cuidadosamente
- Imergir o chip em resina de colofonia aquecida (450C)
- Aquecimento em banho maria (Até diluir o epoxy)
- Filtragem
- Lavagem com água
- Lavagem com acetona concentrada
- Lavagem com isopropanol

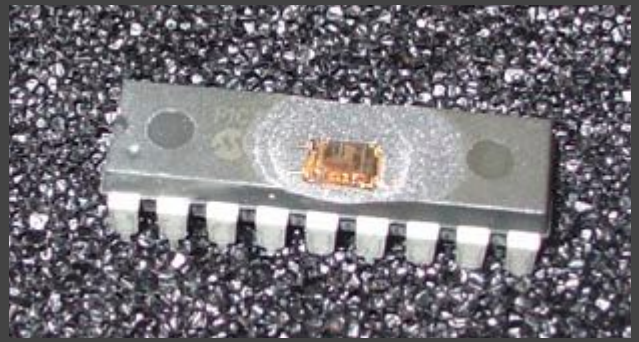


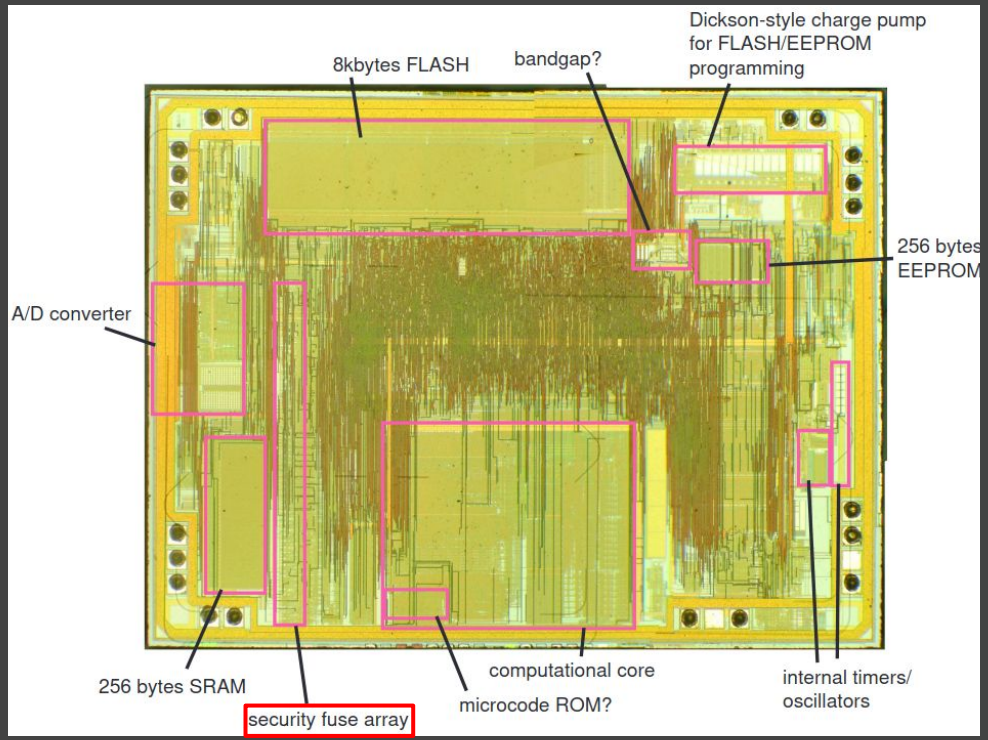
$ A die



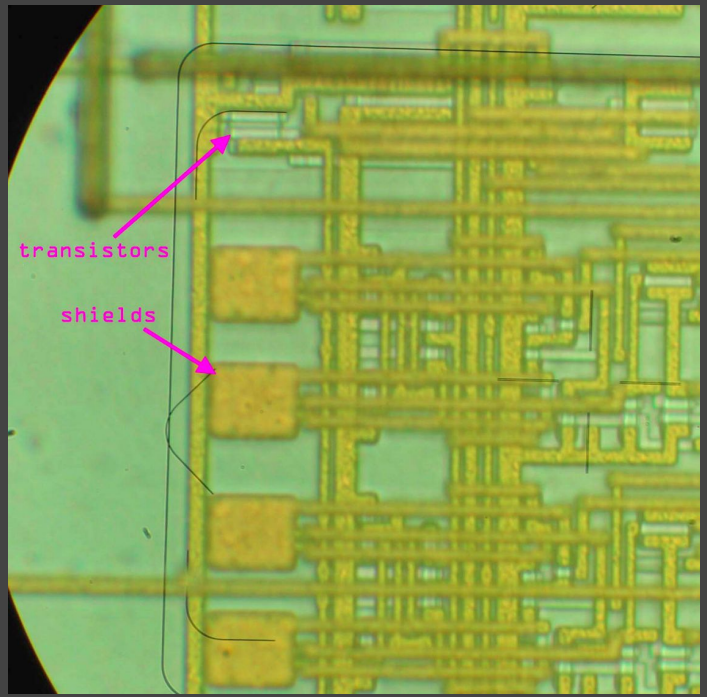


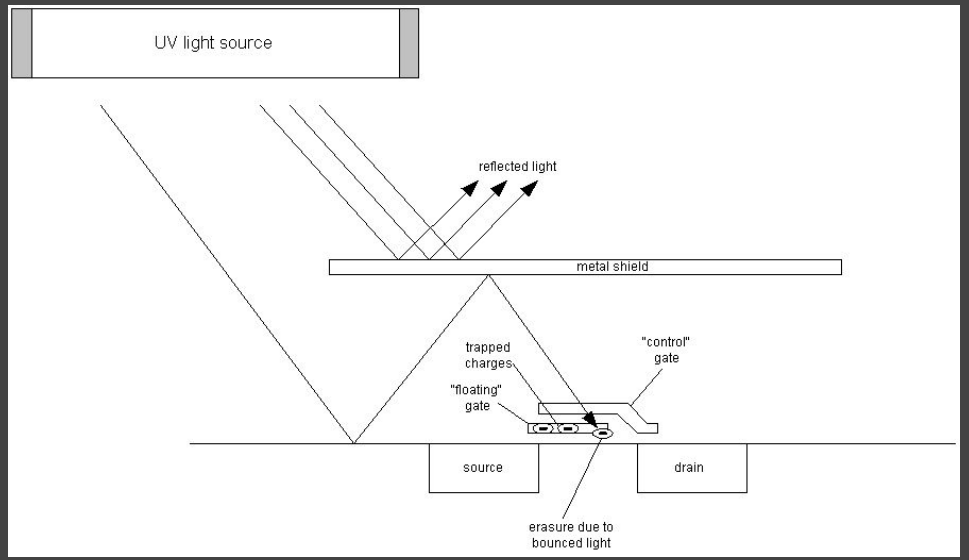
$ Dump de firmware





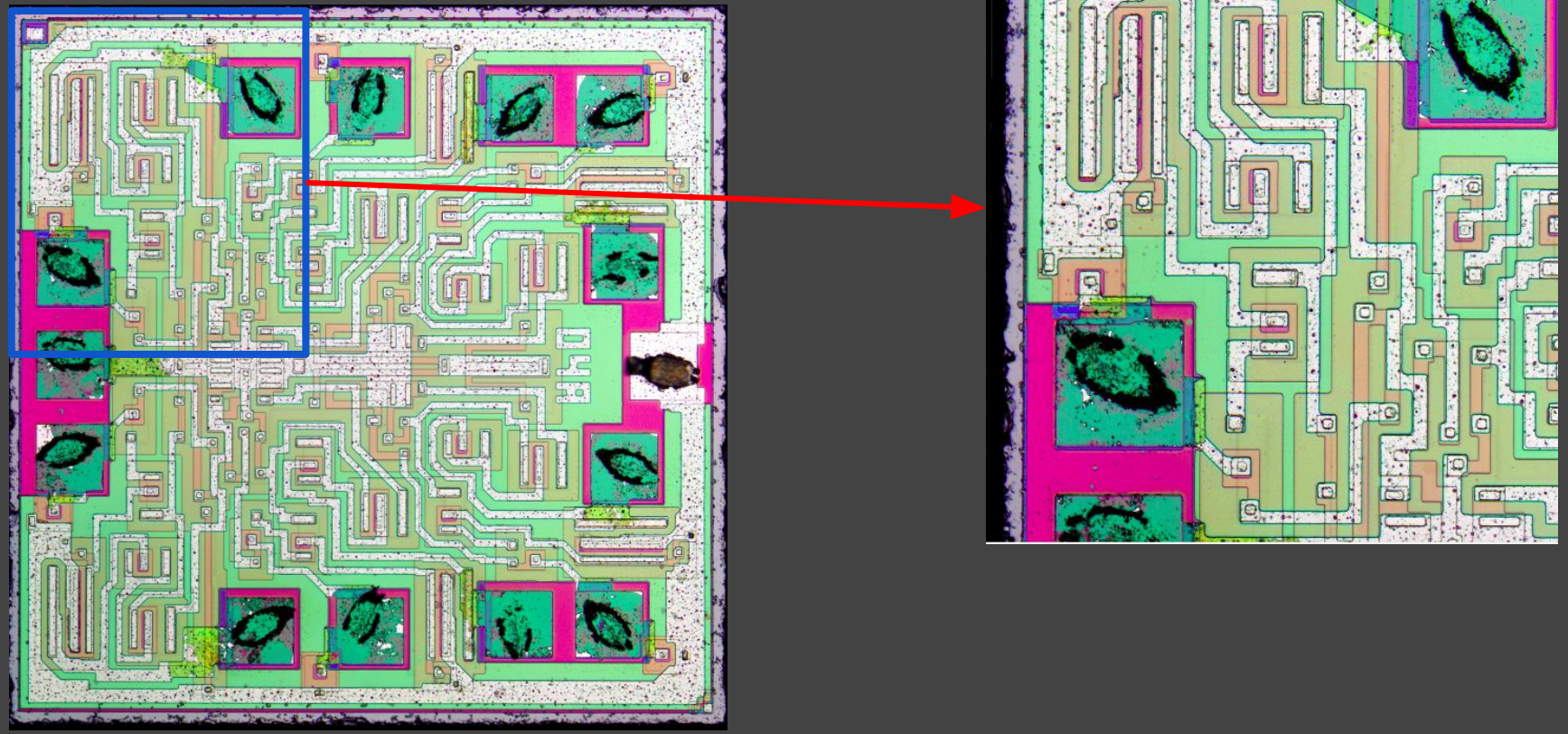
$ Dump de firmware



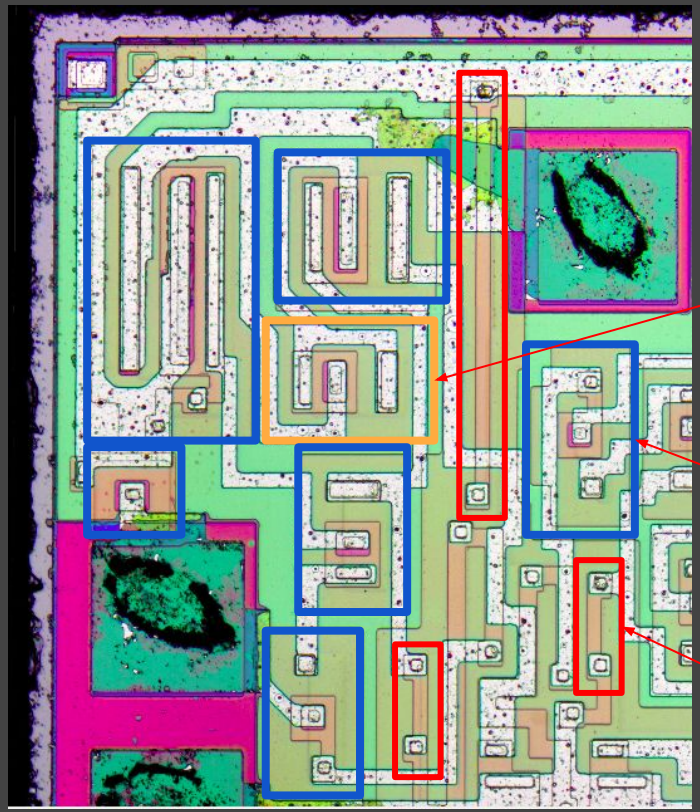


$ Dump de firmware

$ O que está acontecendo aqui?



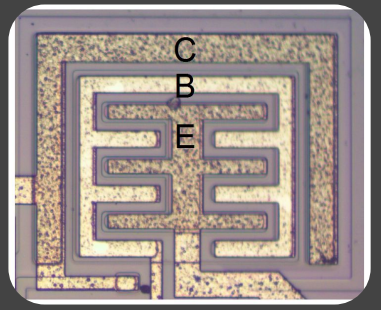
$ O que está acontecendo aqui?

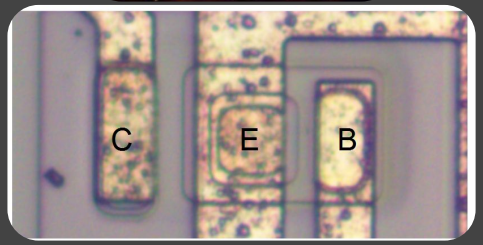


Diodo

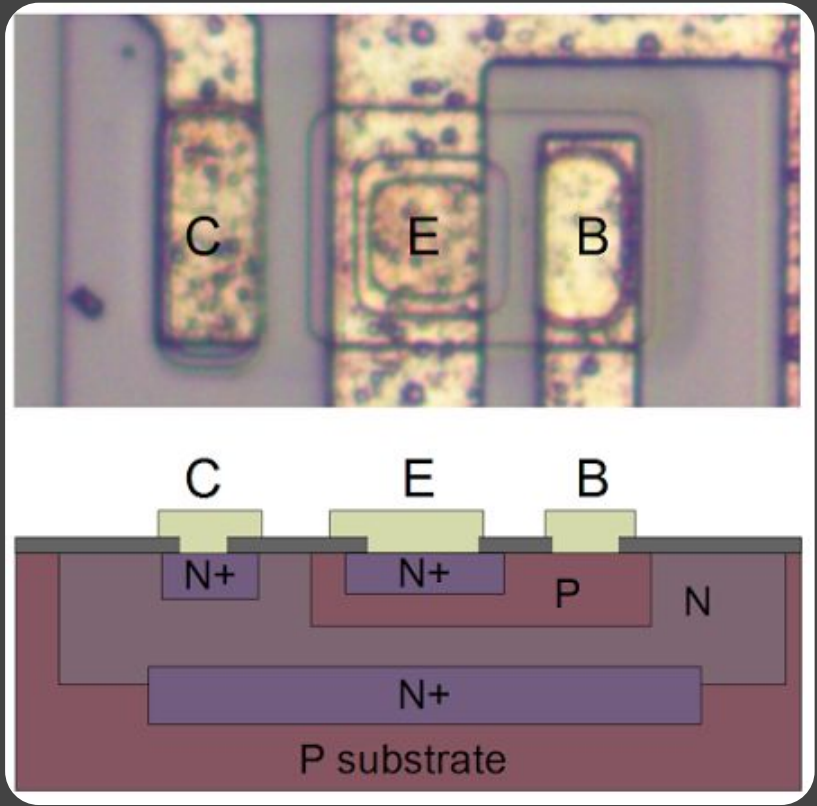
Transistor

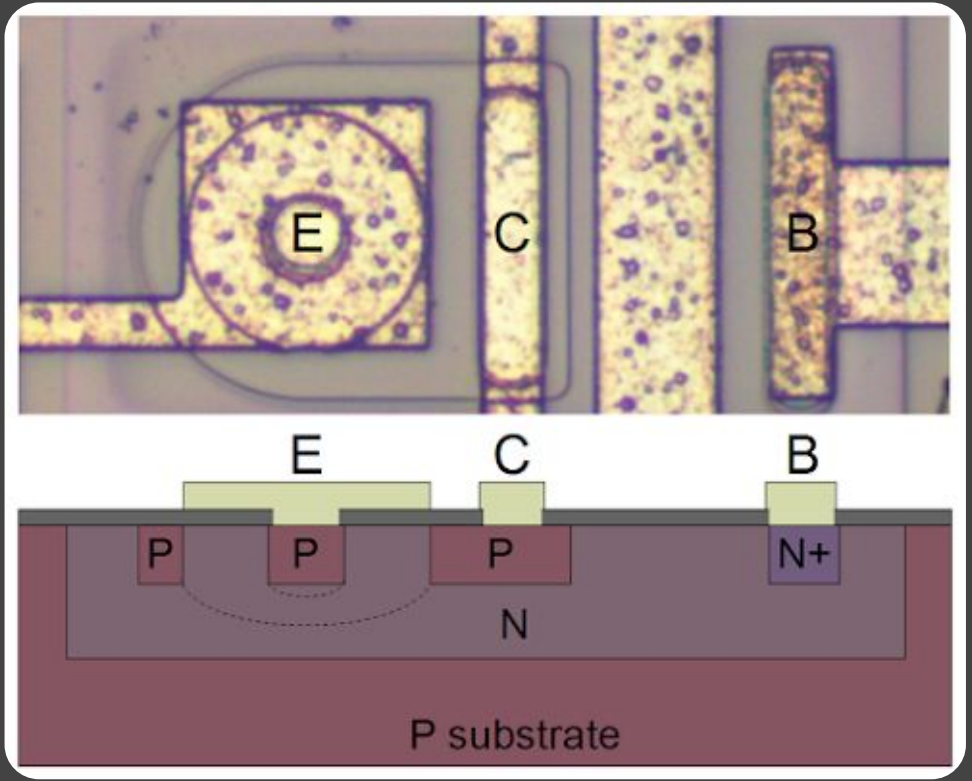
Resistor



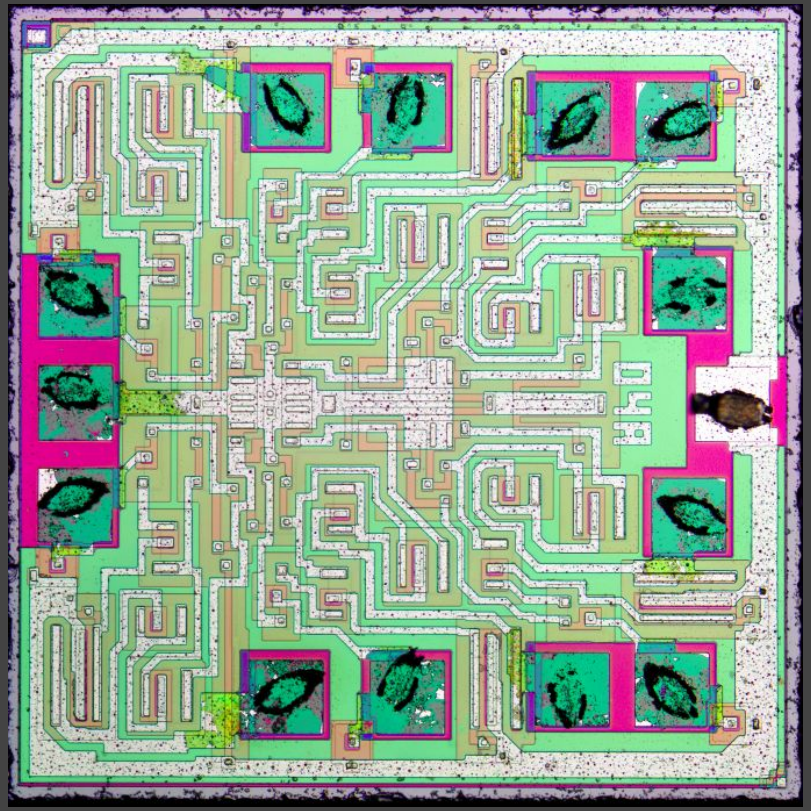


$ Transistor



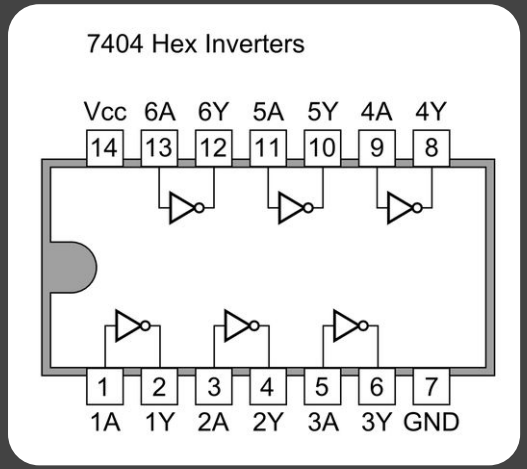


$ Vamos analisar um chip

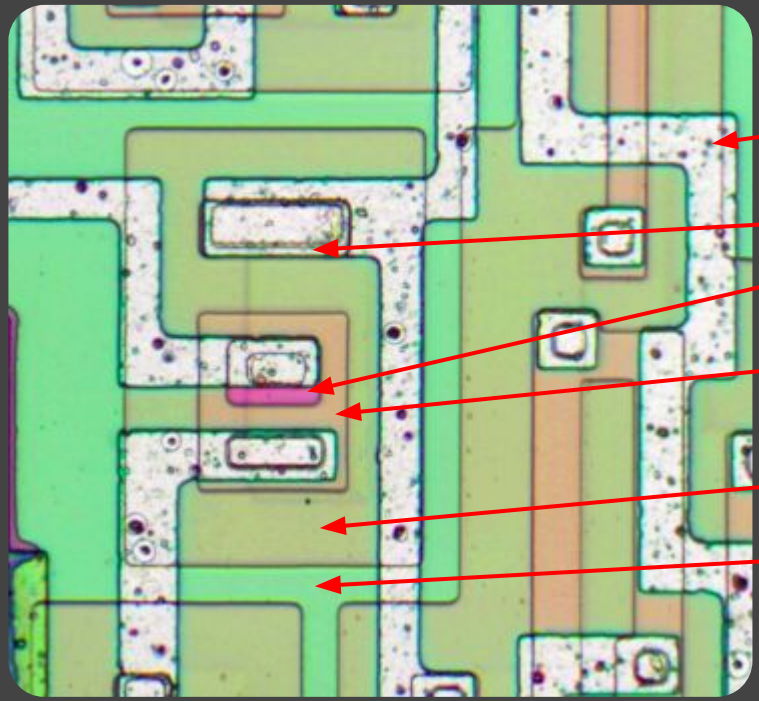


CI 7404: HEX inverter

- 6 portas NOT individuais



$ As camadas



Metal

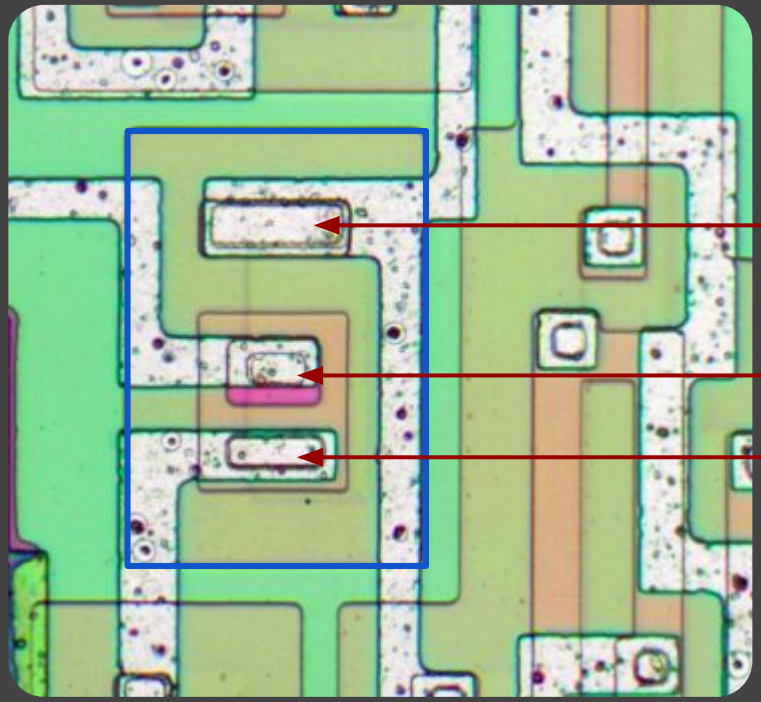
Silício N+

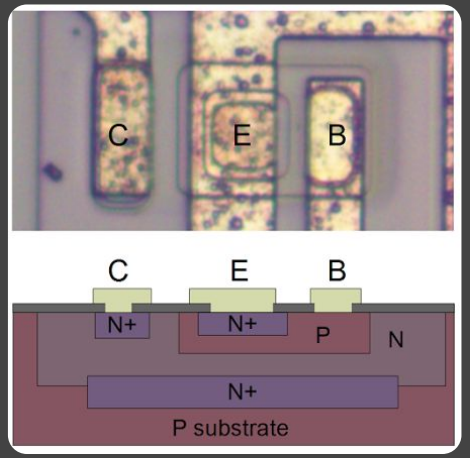
Silício P

Silício N

Silício
Substrato P

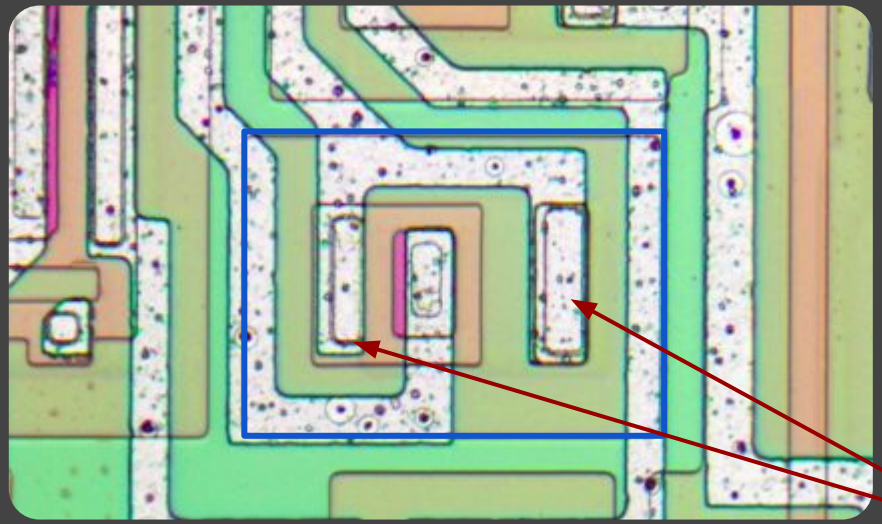
$ O transistor





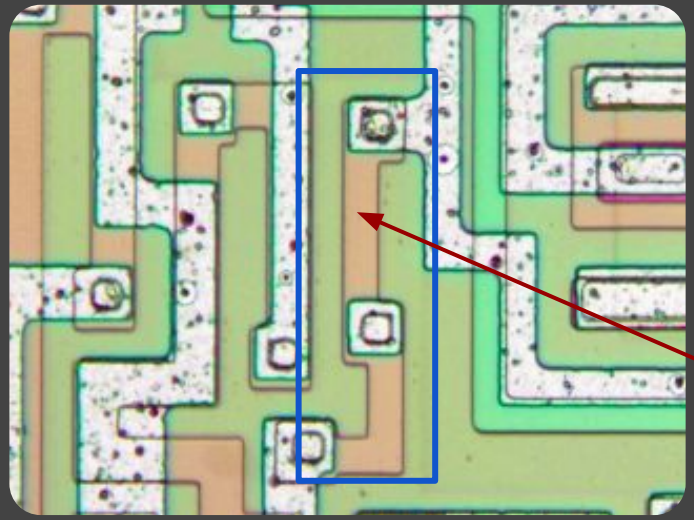
Nosso chip tem apenas transistores NPN (por sorte!)

$ O diodo



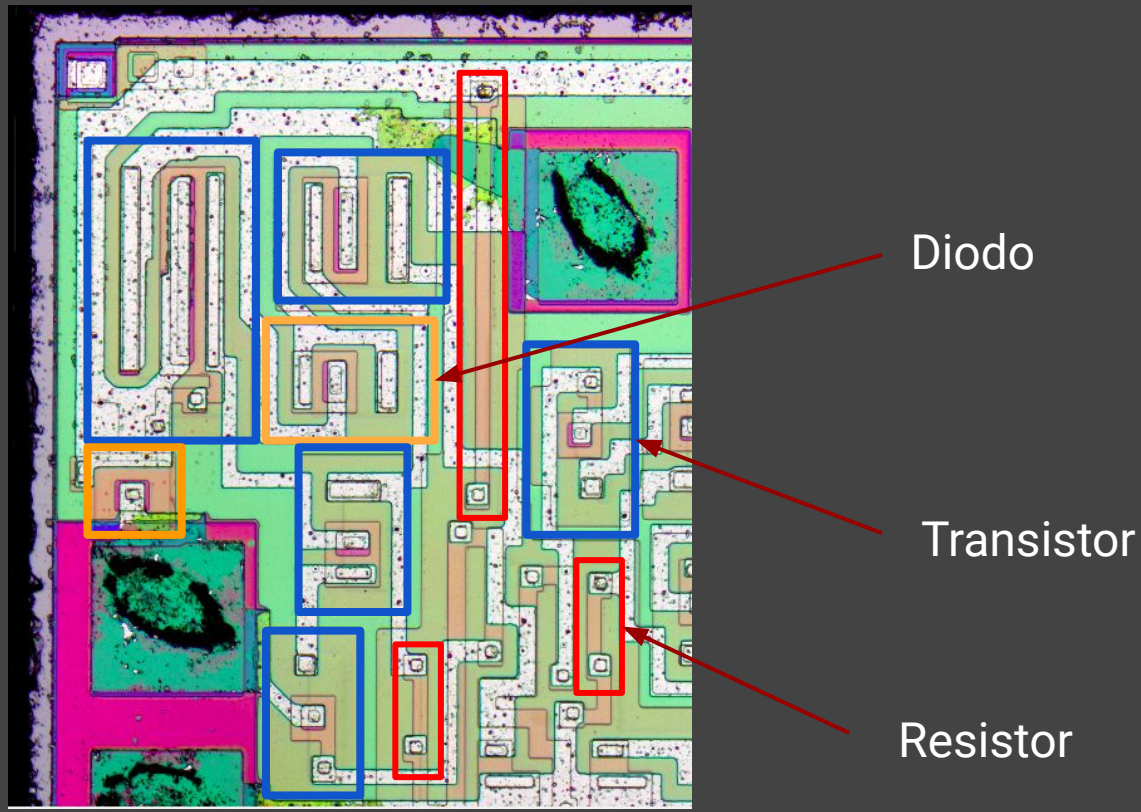
Base e Coletor do transistor NPN interligados formam um diodo

$ O resistor

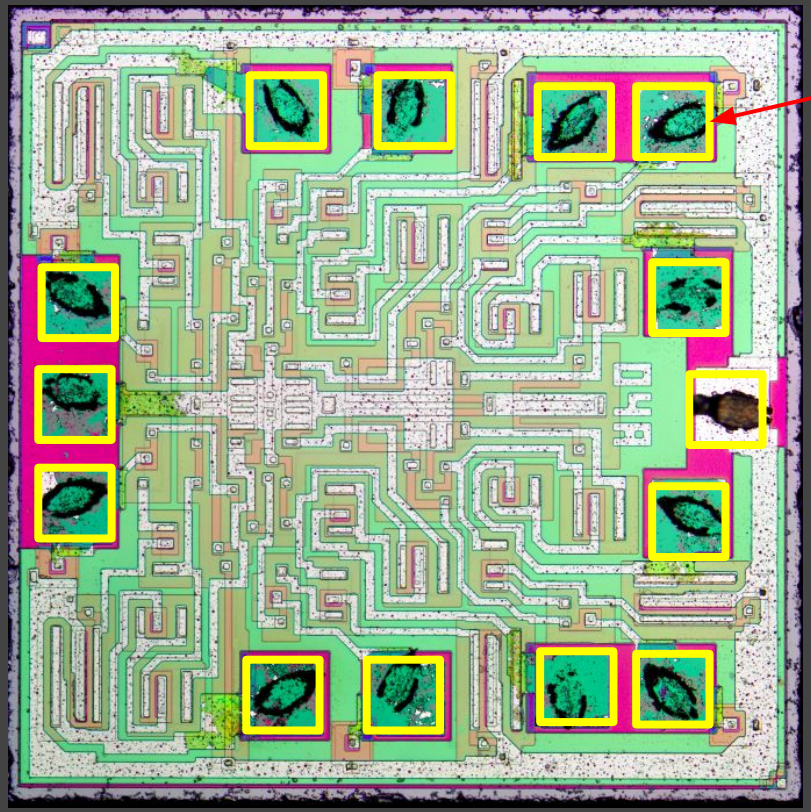


O Resistor é um pedaço de silício P

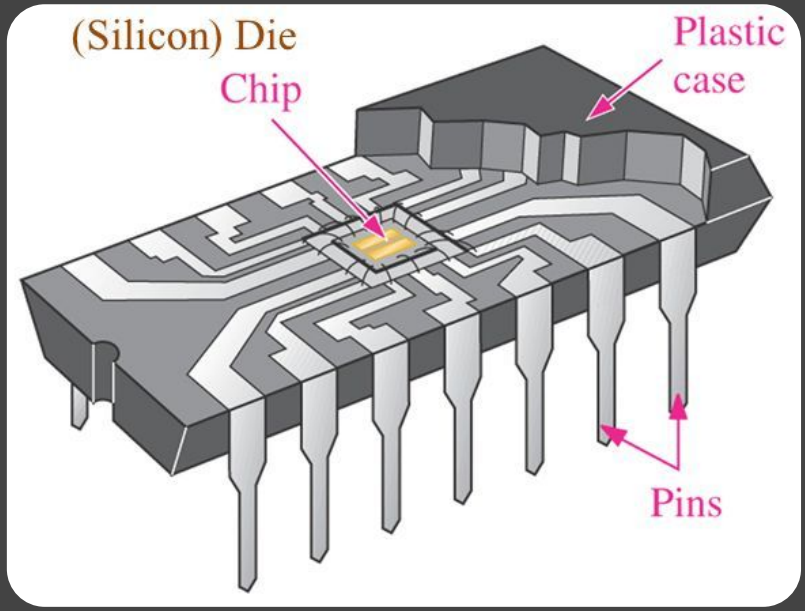
$ Componentes



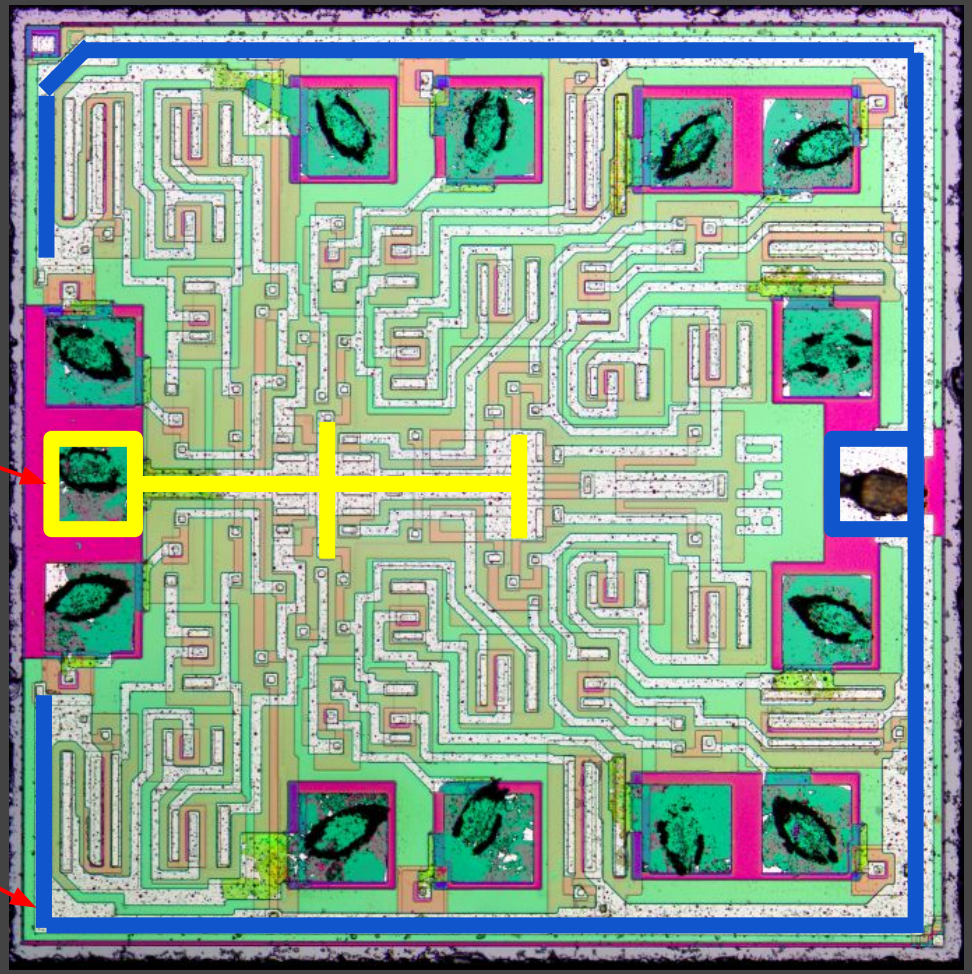
$ As pontes de conexão



Pads

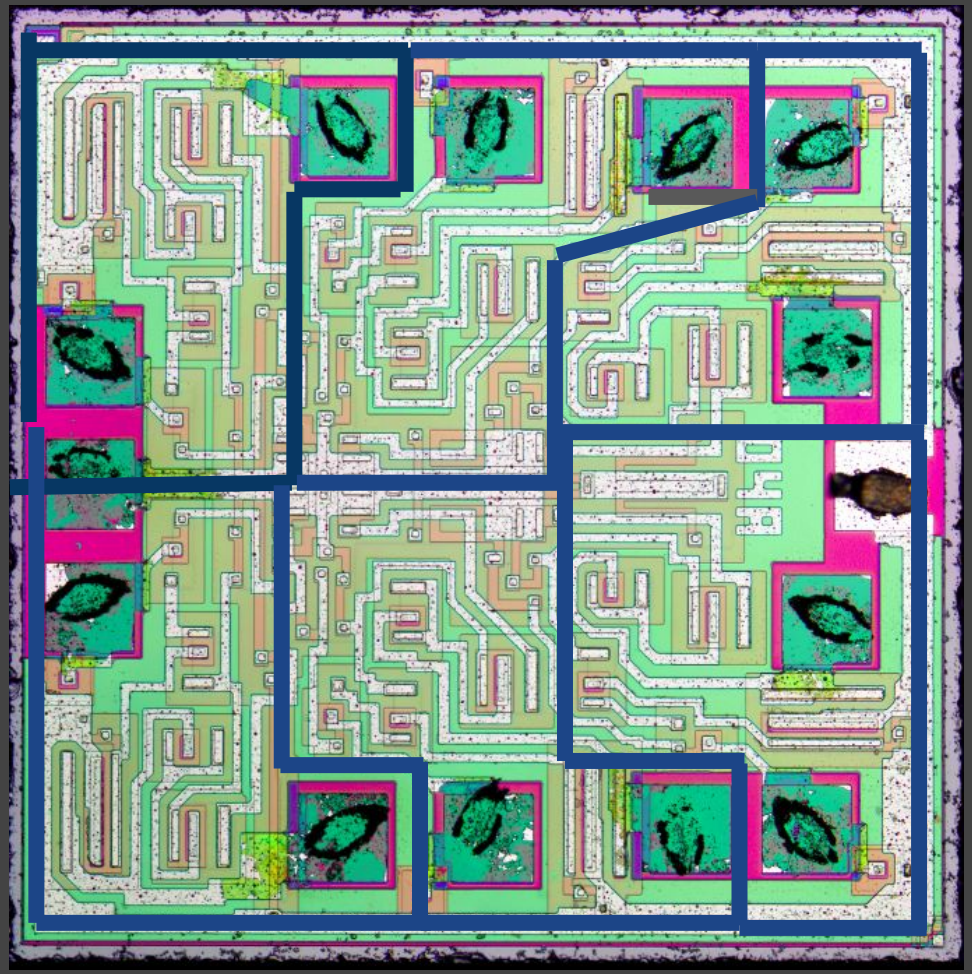


$ Trilhas de energia

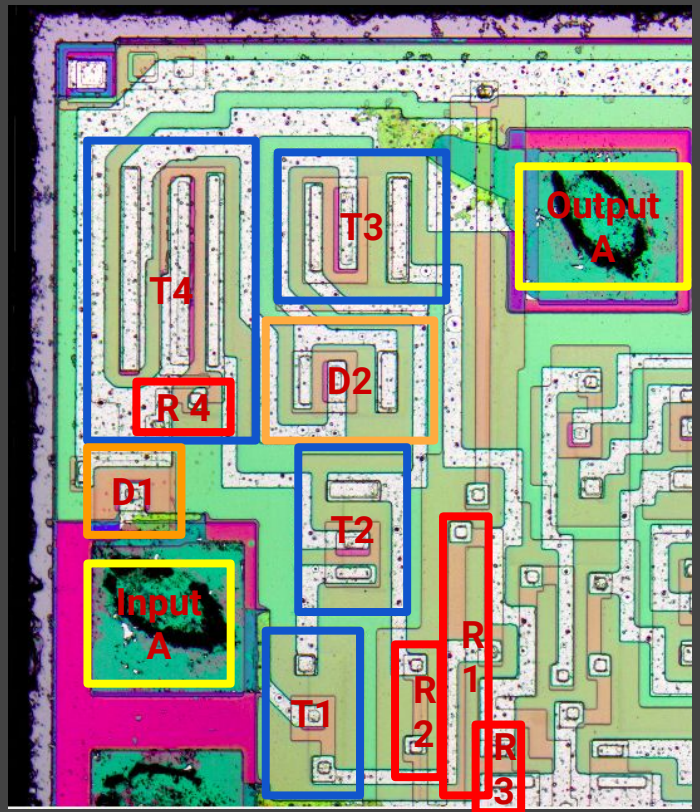


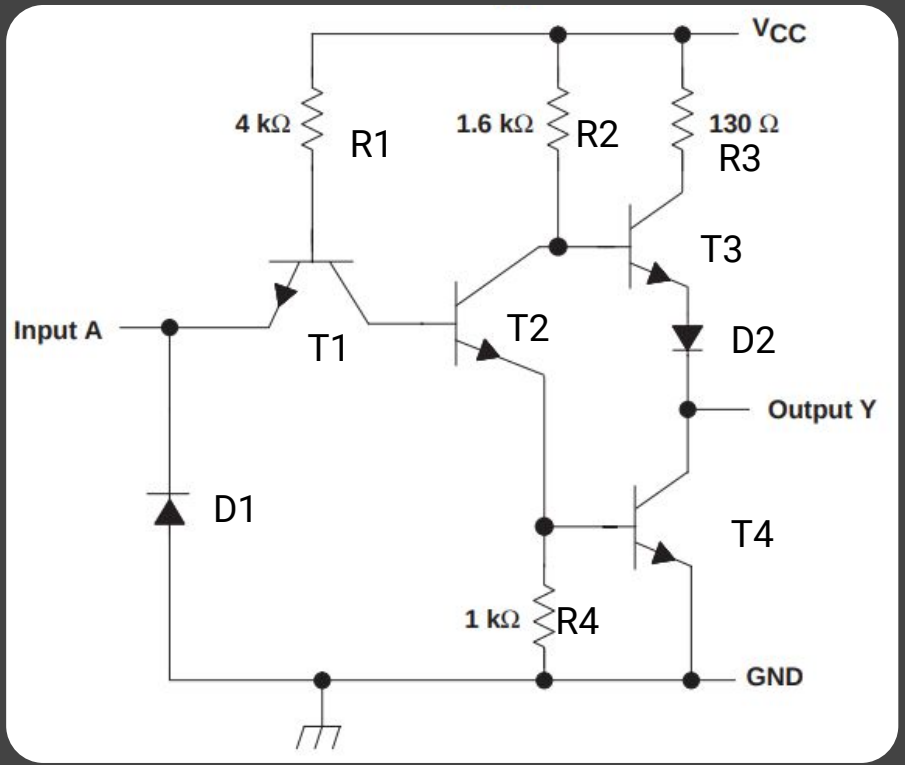
$ Encontrar padrões

Cada divisão é
uma porta
NOT individual



$ Implementação do NOT





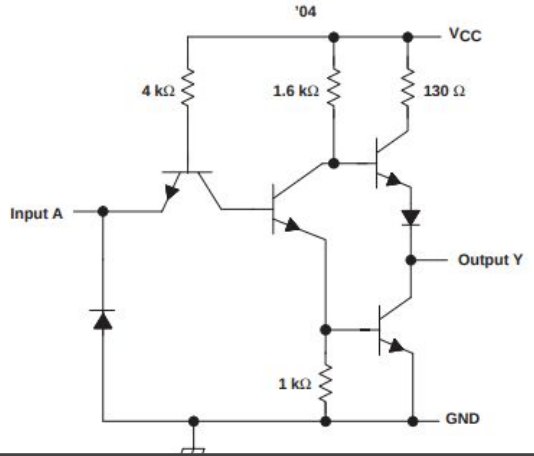
$ Confirmação do datasheet

TEXAS INSTRUMENTS
POST OFFICE BOX 655303 • DALLAS, TEXAS 75265

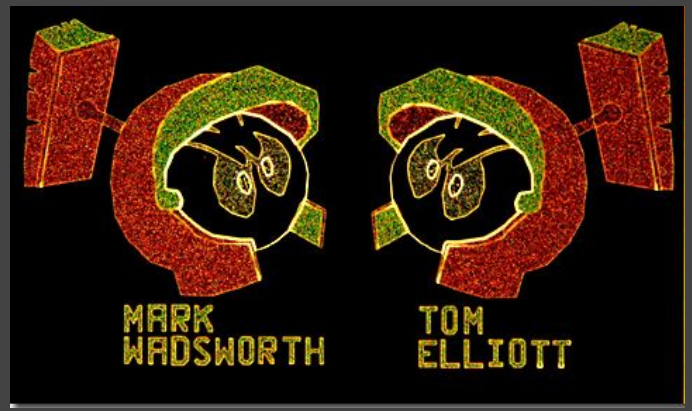
SN5404, SN54LS04, SN54S04,
SN7404, SN74LS04, SN74S04
HEX INVERTERS

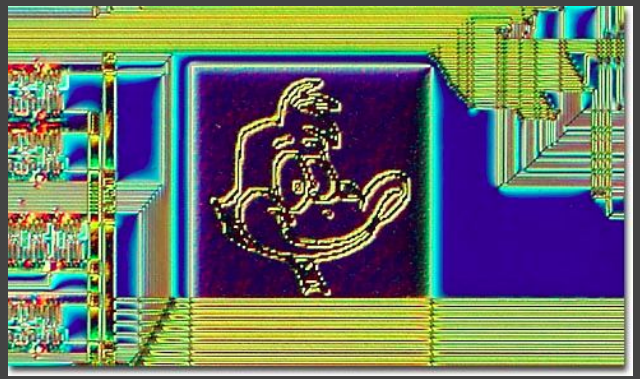
SDLS029C – DECEMBER 1983 – REVISED JANUARY 2004

schematics (each gate)

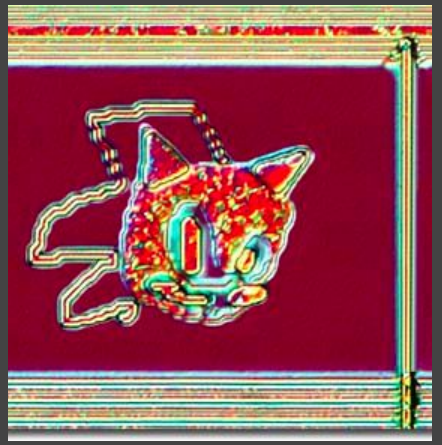


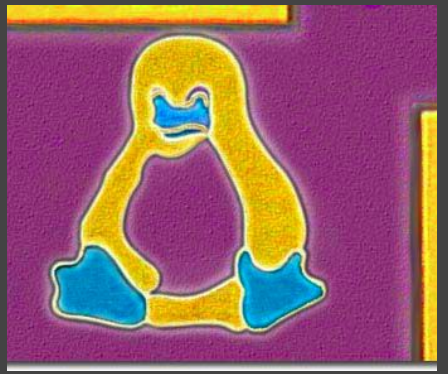
$ Easter Eggs





$ Easter Eggs





$ Referencias

- http://siliconpr0n.org/
- http://www.righto.com/
- http://www.eevblog.com/
- https://www.youtube.com/watch?v=IcrBqCFLHIY
- http://www.t4f.org/articles/ultra-low-cost-ic-decapsulation/
- http://www.ti.com/lit/ds/symlink/sn54ls04-sp.pdf
- https://swarup.ece.ufl.edu/papers/IC/IC6.pdf
- https://ieeexplore.ieee.org/document/8268780
- https://ryancor.medium.com/hardware-trojans-under-a-microscope-bf542acbcc29
- https://www.bunniestudios.com/blog/hacking-the-pic-18f1320/
- https://www.youtube.com/watch?v=UDoXOatvIsg
- http://uvicrec.blogspot.com/2010/04/ic-decapping-round-2.html
- https://www.youtube.com/watch?app=desktop&v=mT1FStxAVz4
- http://uvicrec.blogspot.com/2010/04/ic-decapping-round-2.html
- https://www.reddit.com/r/ReSilicon/
- https://cordis.europa.eu/article/id/435845-understanding-and-preventing-the-malicious-hardware-trojan

Engenharia reversa *in Silico*

Desmistificando o Silício

https://tinyurl.com/revsilico