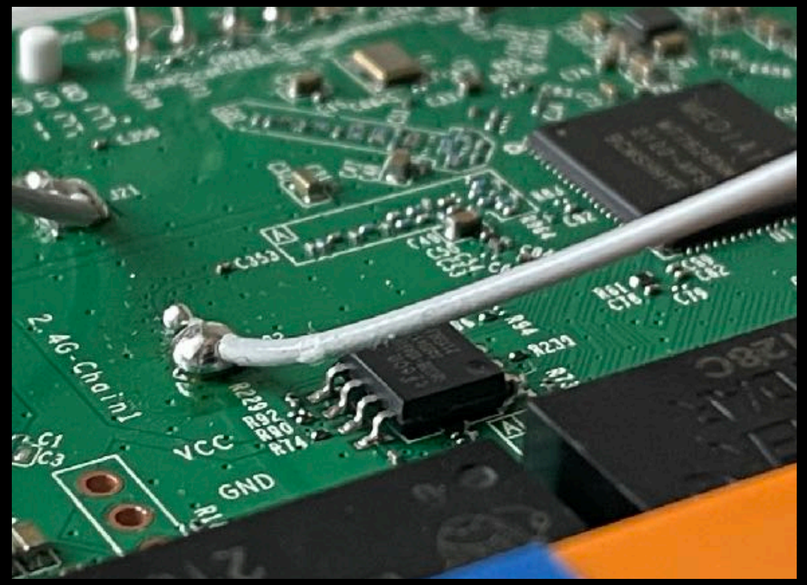
Physical Attacks

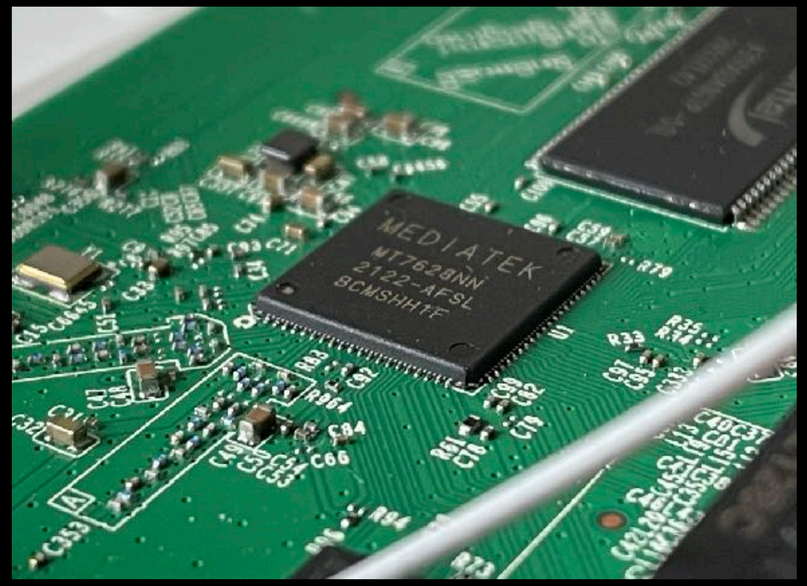
MIT 6.888 Spring 2022

Mengjia Yan & Joseph Ravichandran

Image: Proto G Engineering, "Oscilloscope Art"

Who do you trust?





What if the **user** is the attacker?

Physical Attacks

Direct access to a chip is possible: signals can be injected, modified, or measured

XBOX

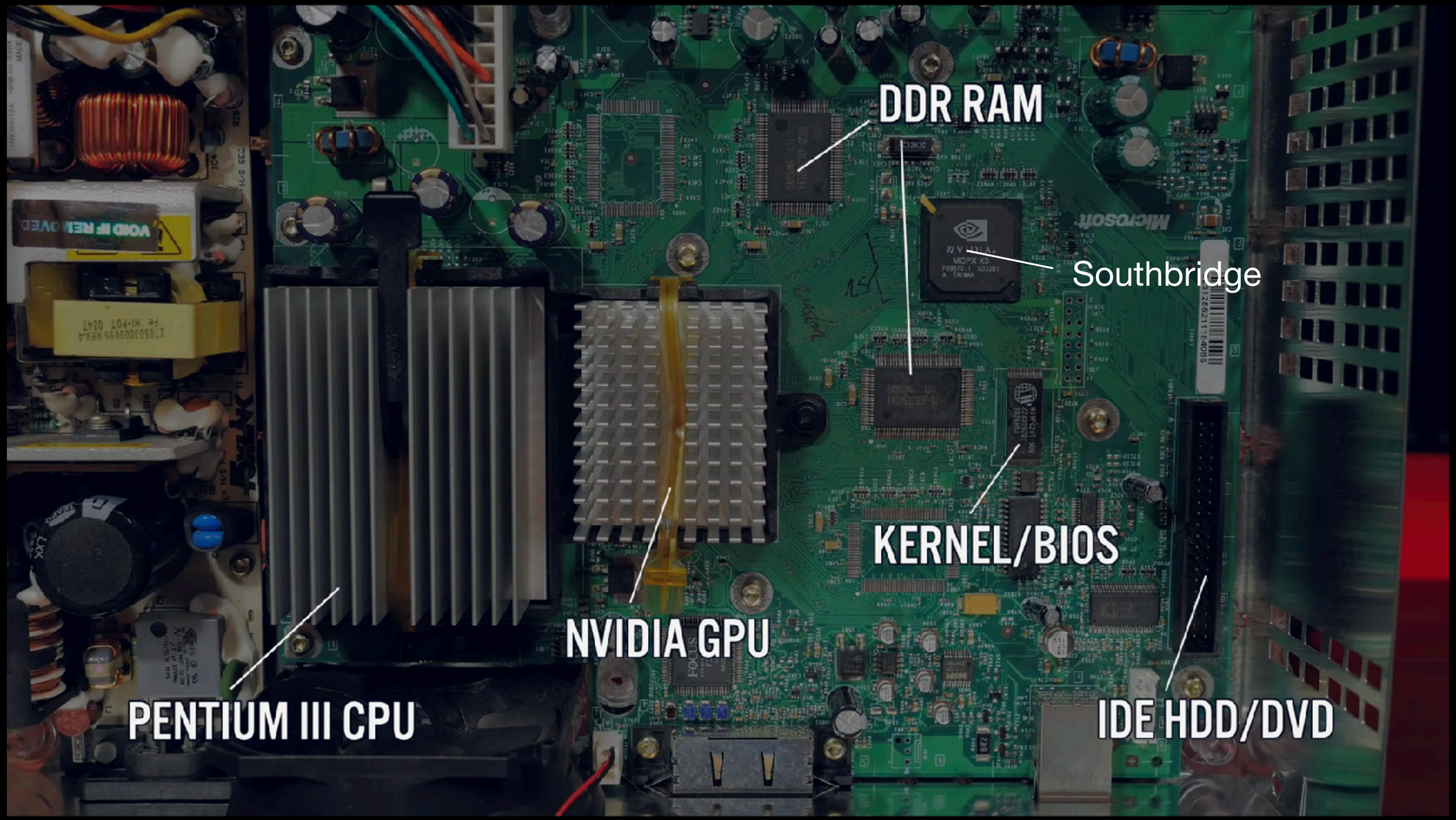
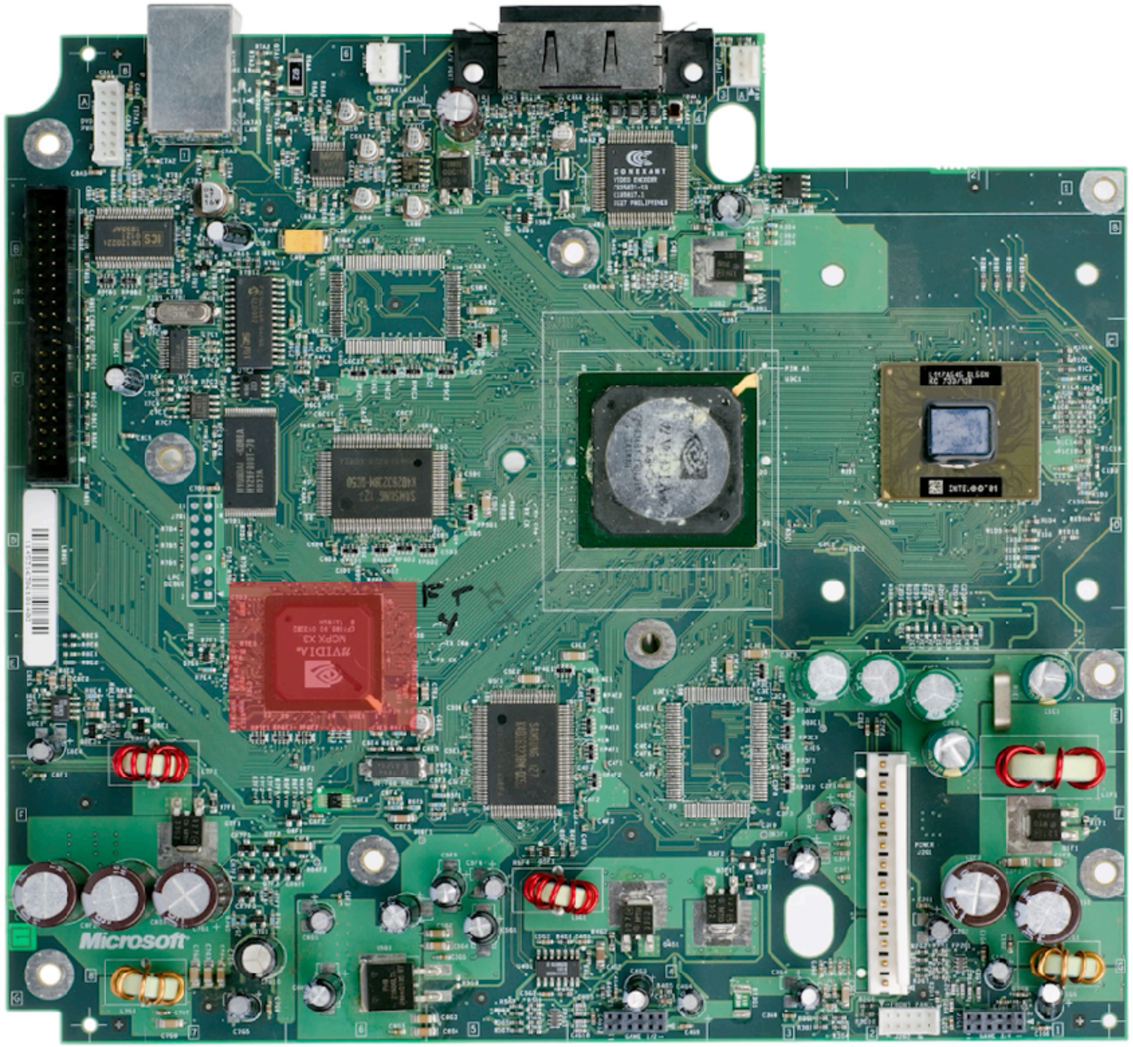


Image: Modern Vintage Gamer (YouTube)



- "SECRET ROM" STORED IN MCPX
- FLASH DECRYPTION KEY (RC4) STORED IN "SECRET ROM"

Image: Modern Vintage Gamer (YouTube)

Active

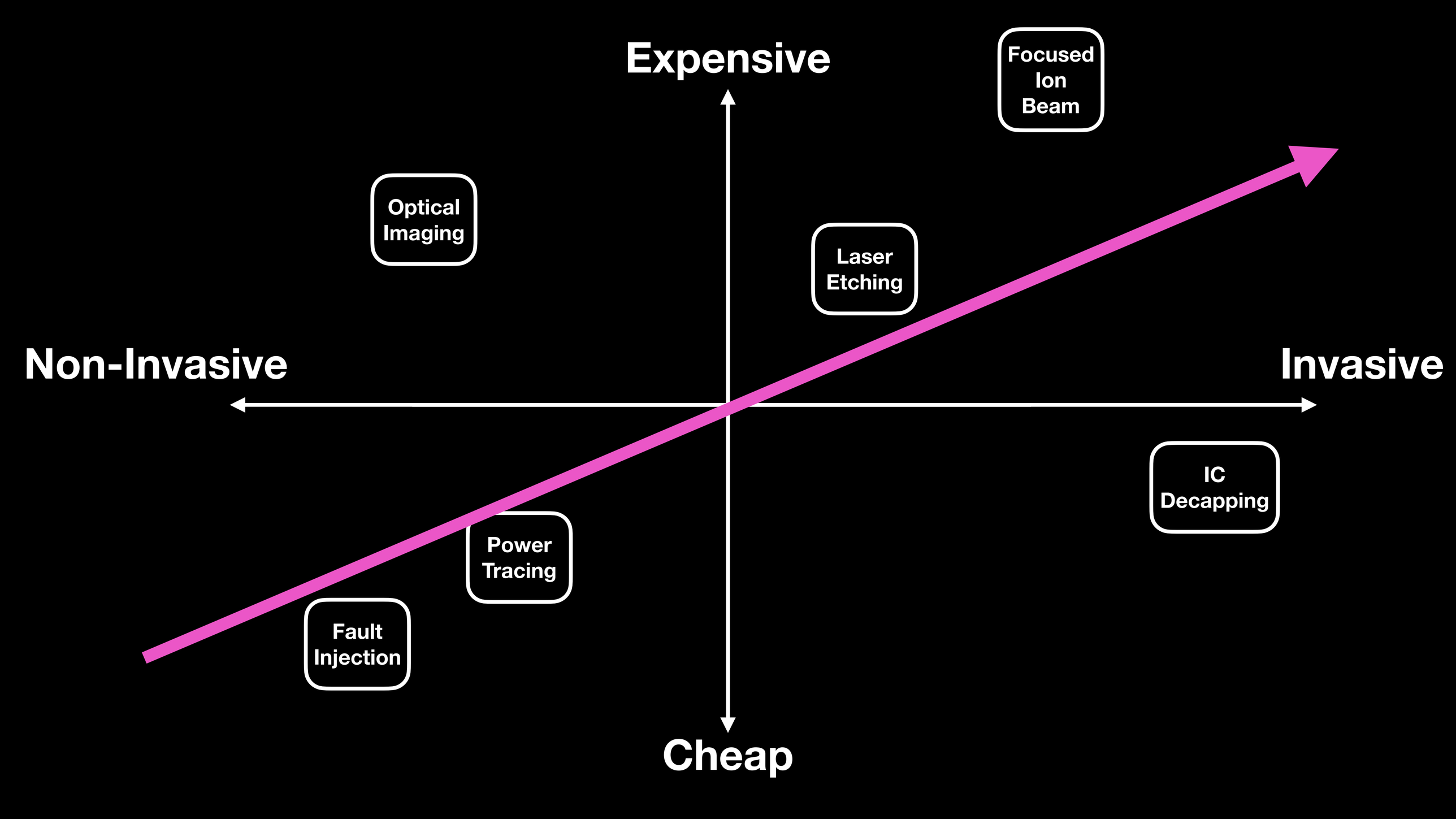
Inject new signals

Modify existing signals in new ways

Passive

No modification of signals

Only observe regular operation


Expensive
Focused Ion Beam
Optical Imaging
Laser Etching
Non-Invasive
Invasive
IC Decapping
Power Tracing
Fault Injection
Cheap

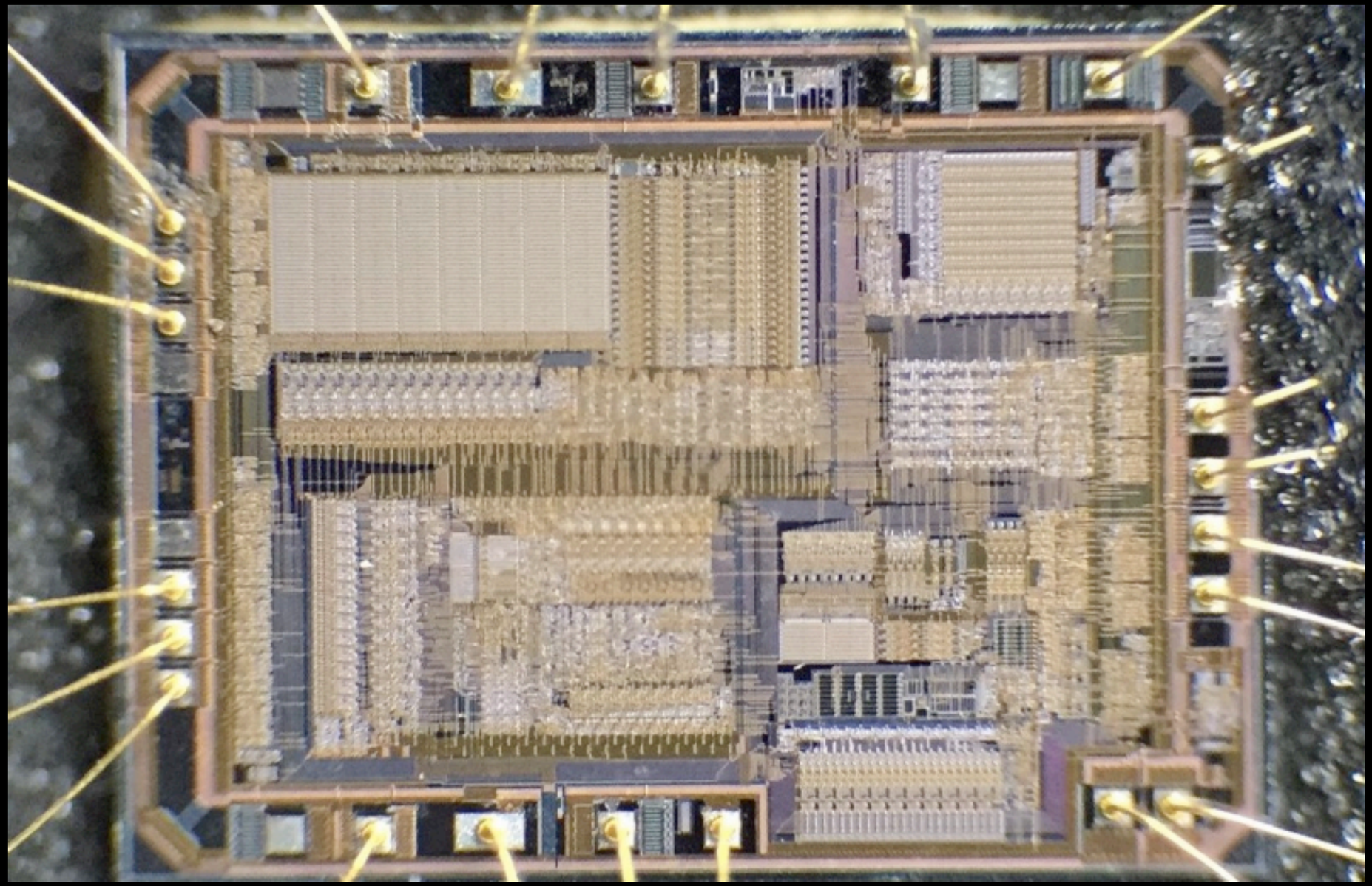


Image: Hackaday

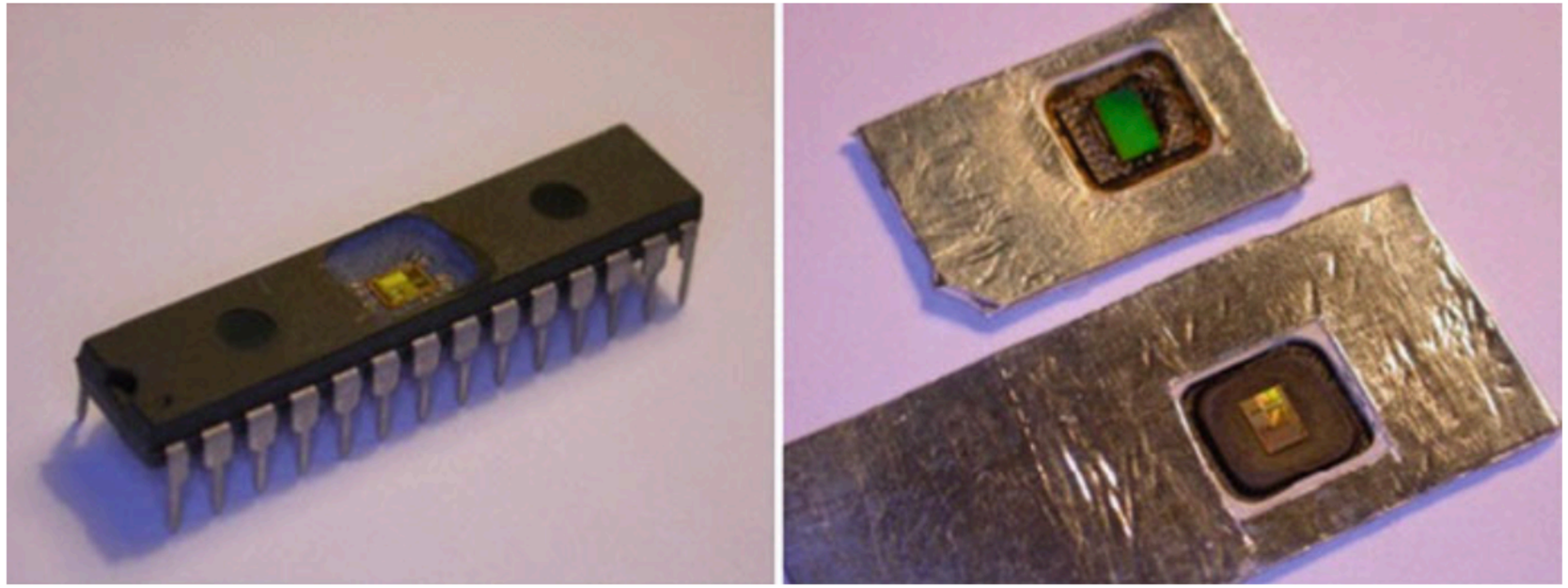


Fig. 7.3 Decapsulated chips

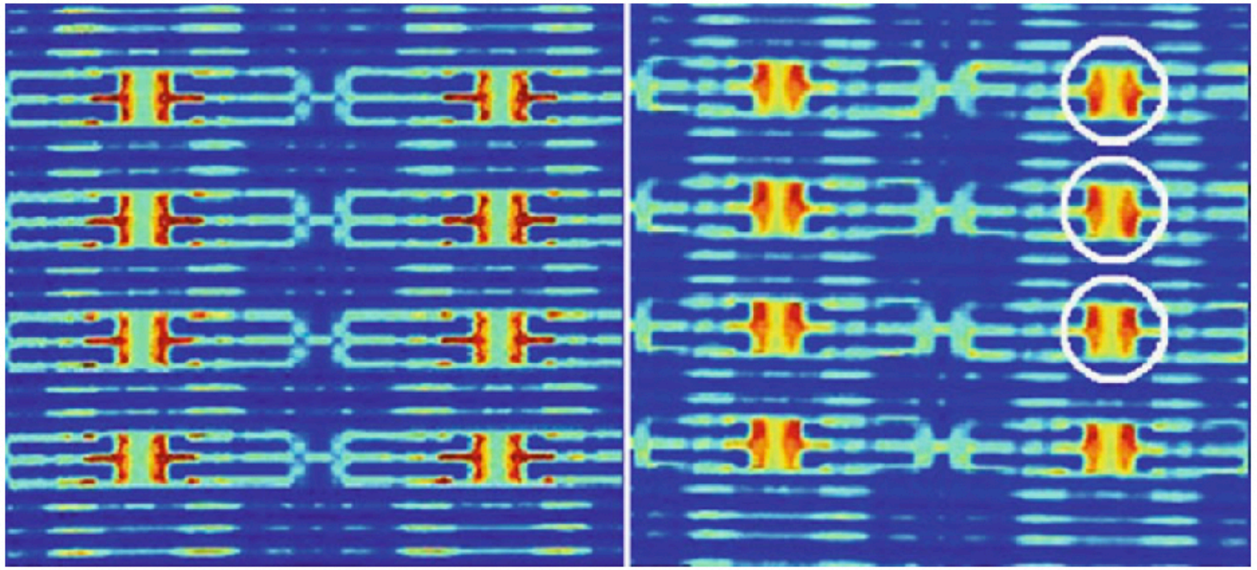


Fig. 7.6 Laser scan of unpowered and powered-up SRAM in PIC16F84 microcontroller

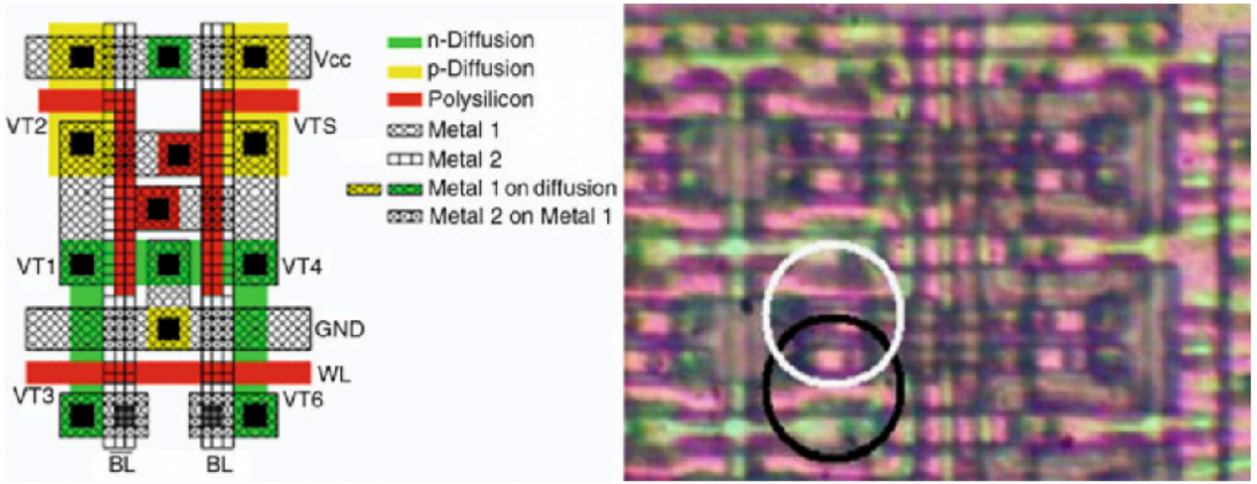


Fig. 7.7 Layout of SRAM cell and SRAM area in PIC16F84 microcontroller

Some Common Terms

JTAG

Joint Test Action Group: A debug interface for testing devices. If this is left enabled on a product, you can do fun things. See: J-Link, Jtagulator.

SWD

Single Wire Debug: The ARM debugger protocol built on JTAG. Think GDB but for embedded systems. May be disabled by security bit (this can be glitched).

Flash

(Sometimes Builtin) storage that the microcontroller uses to store firmware, code, data, etc. If external, can be dumped. May be encrypted.

Security Bit

Setting that disables code readout on an MCU. Allows manufacturers to leave debug ports (like SWD) on the PCB without worrying about us dumping their code. Can be glitched.

Boot ROM

Read-only code that initiates CPU bringup. This is fixed in silicon and cannot be modified. Bugs here are nearly always catastrophic for system security.

4 Attacks

Today

Fault Injection

Power Analysis

Coldboot

Timing Analysis

Active

Fault Injection

Coldboot

Passive

Power Analysis

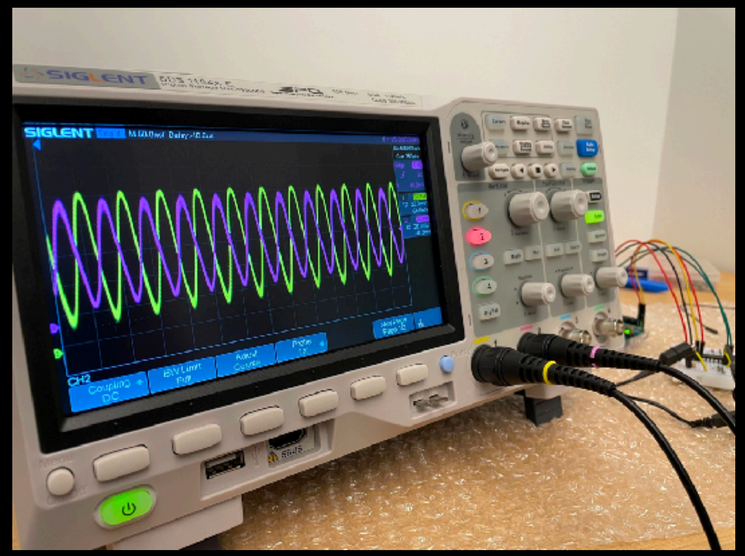
Timing Analysis

Fault Injection

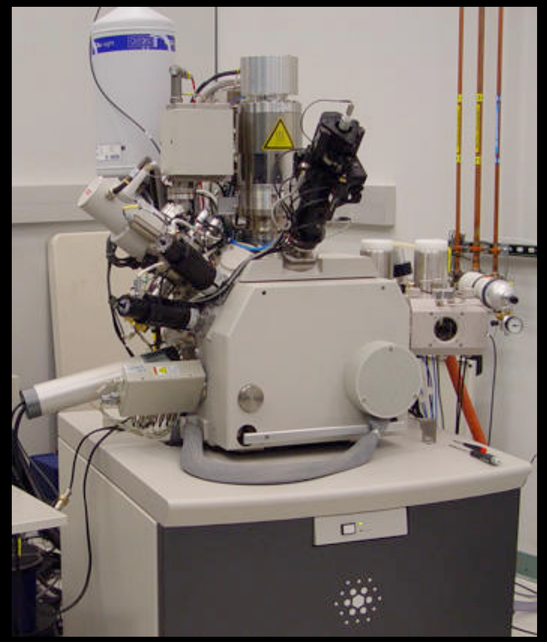
Tools

Cheap

Affordable



Crazy Expensive



Yes, Really

hackaday.com

HACKADAY

HOME BLOG HACKADAY.IO TINDIE HACKADAY PRIZE SUBMIT ABOUT

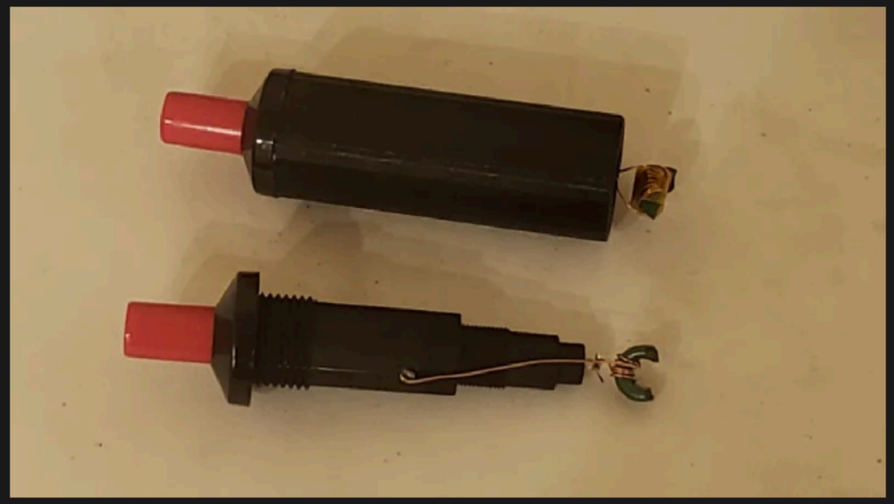
March 8, 2022

BLAST CHIPS WITH THIS BBQ LIGHTER FAULT INJECTION TOOL

by: Dan Maloney

16 Comments

January 29, 2022

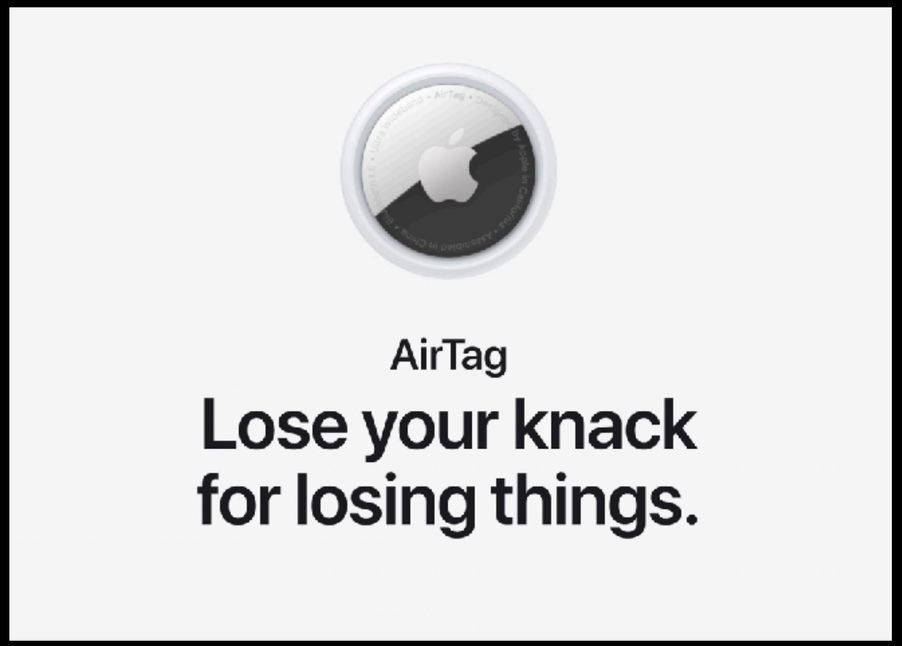


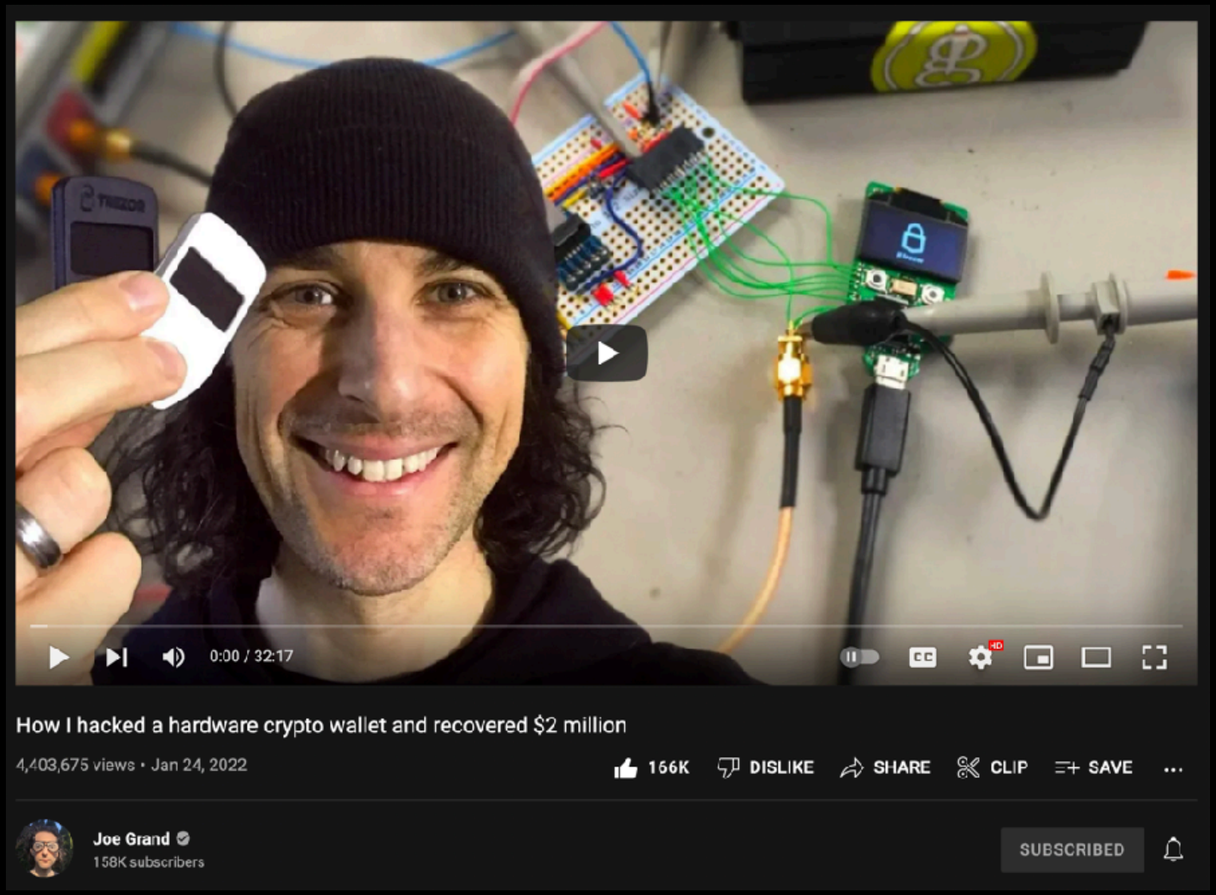
Looking to get into fault injection for your reverse engineering projects, but don't have the cash to lay out for the necessary hardware? Fear not, for the tools to glitch a chip may be as close as the nearest barbecue grill.

SEARCH

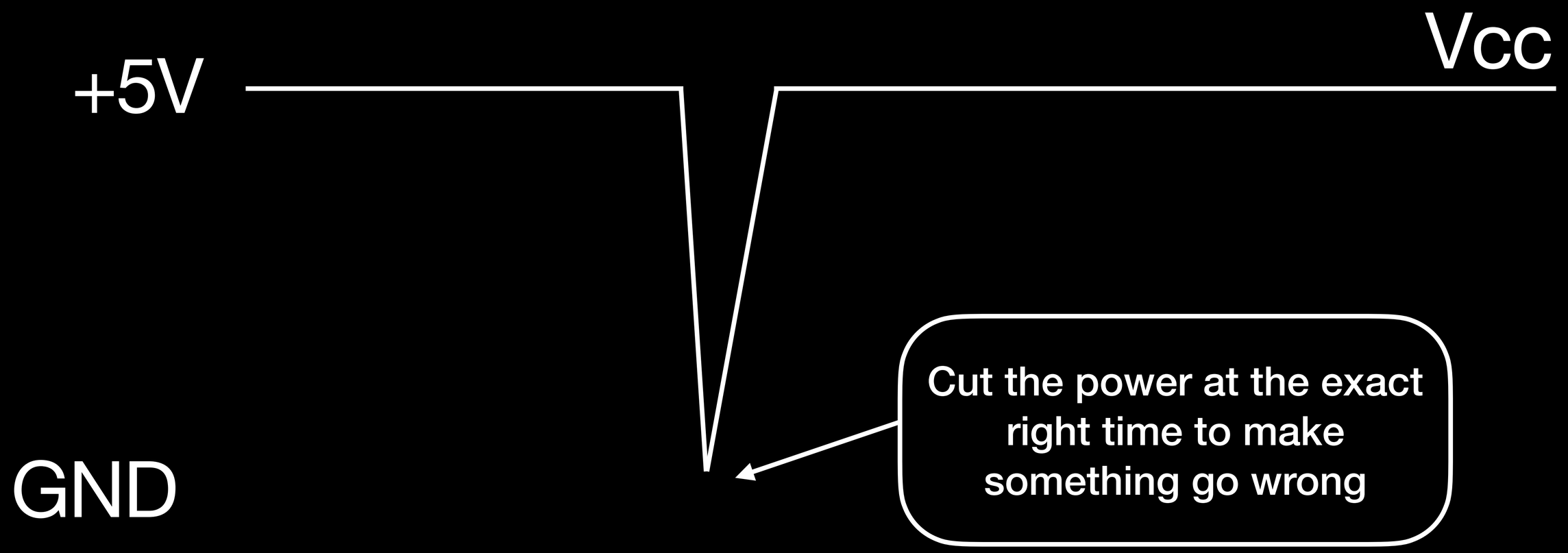
Search ... SEARCH

Notable Examples





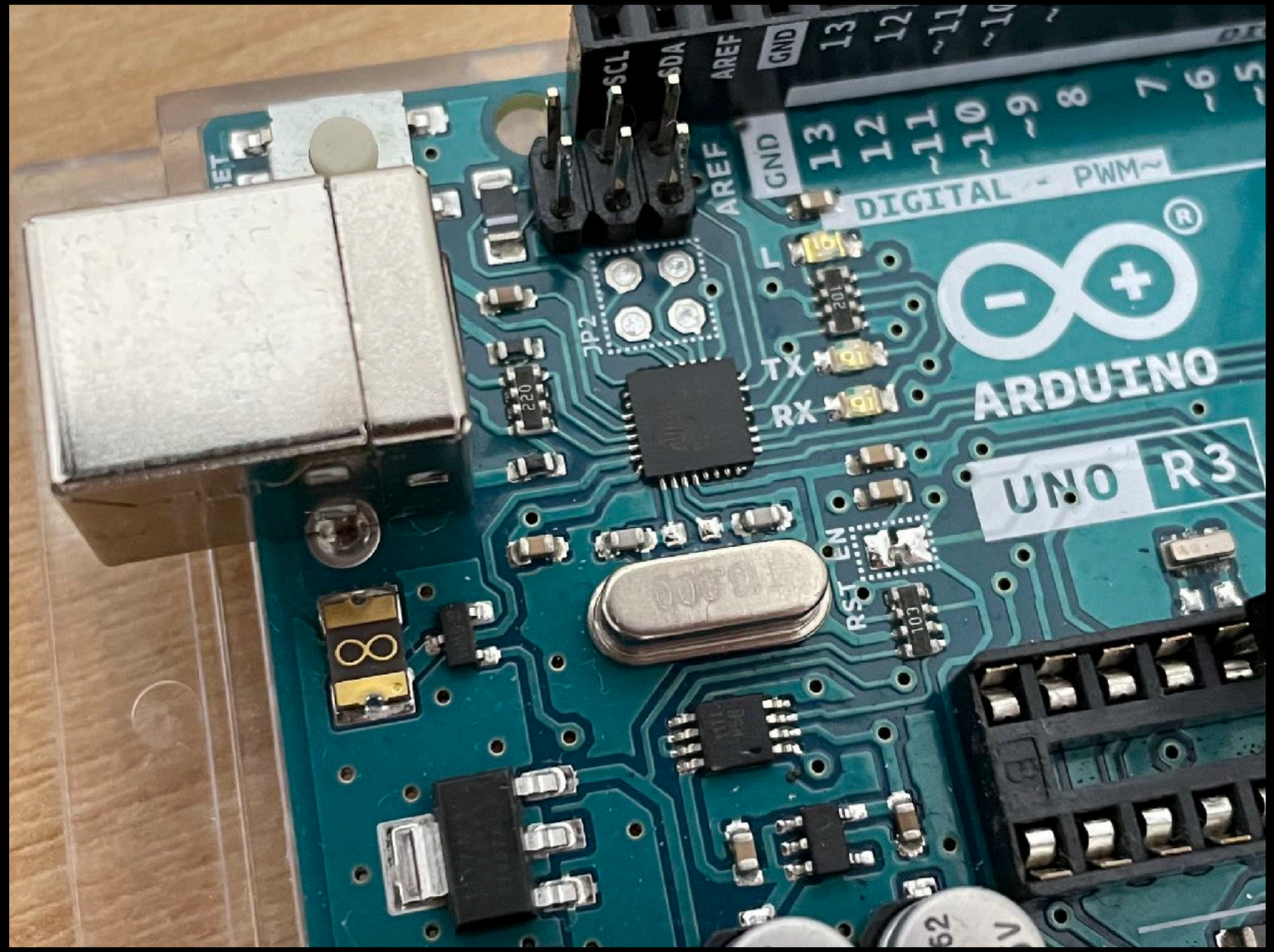
Voltage Glitching

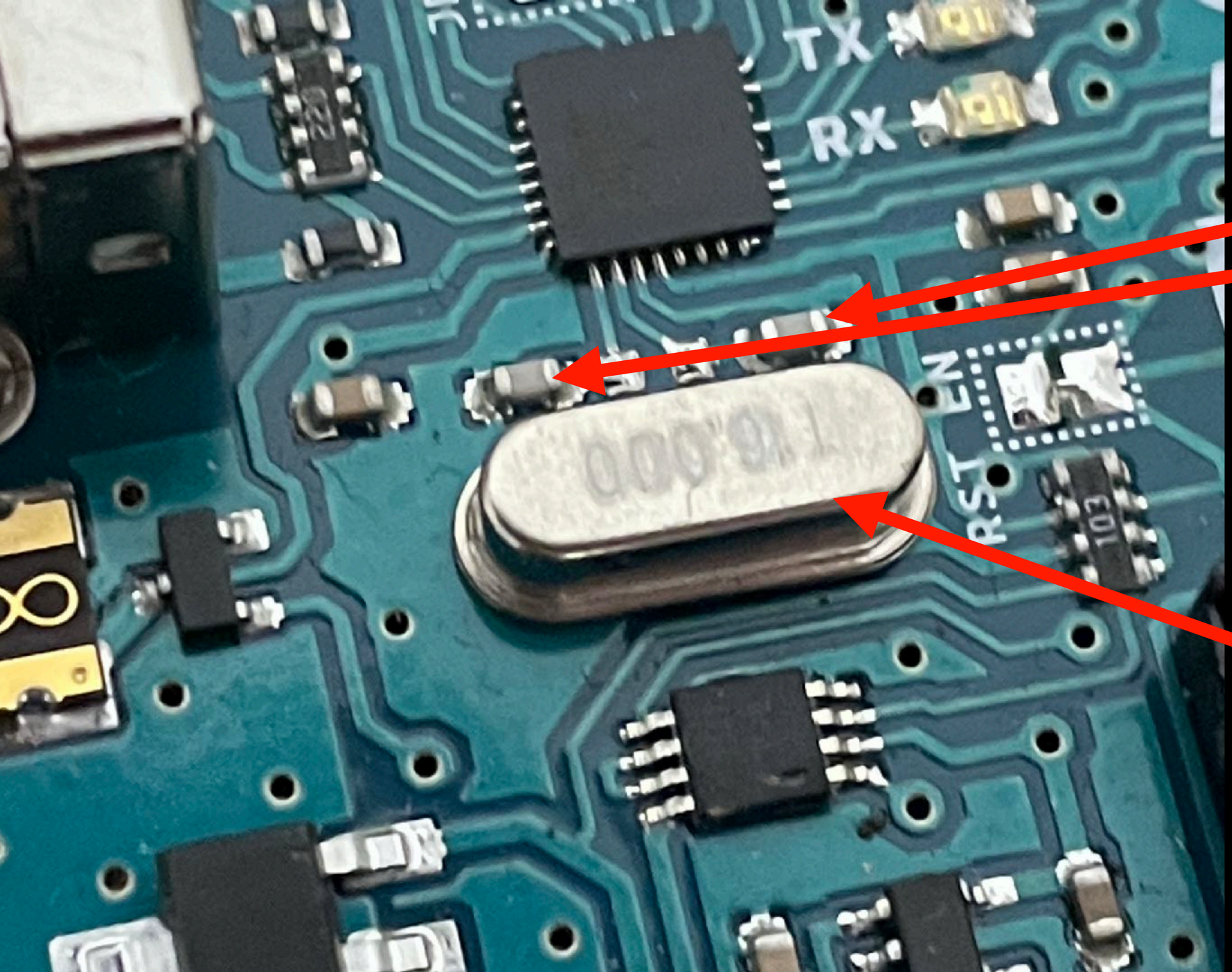


Voltage Glitching

Challenge

Need to deal with capacitors, which filter out our attack.

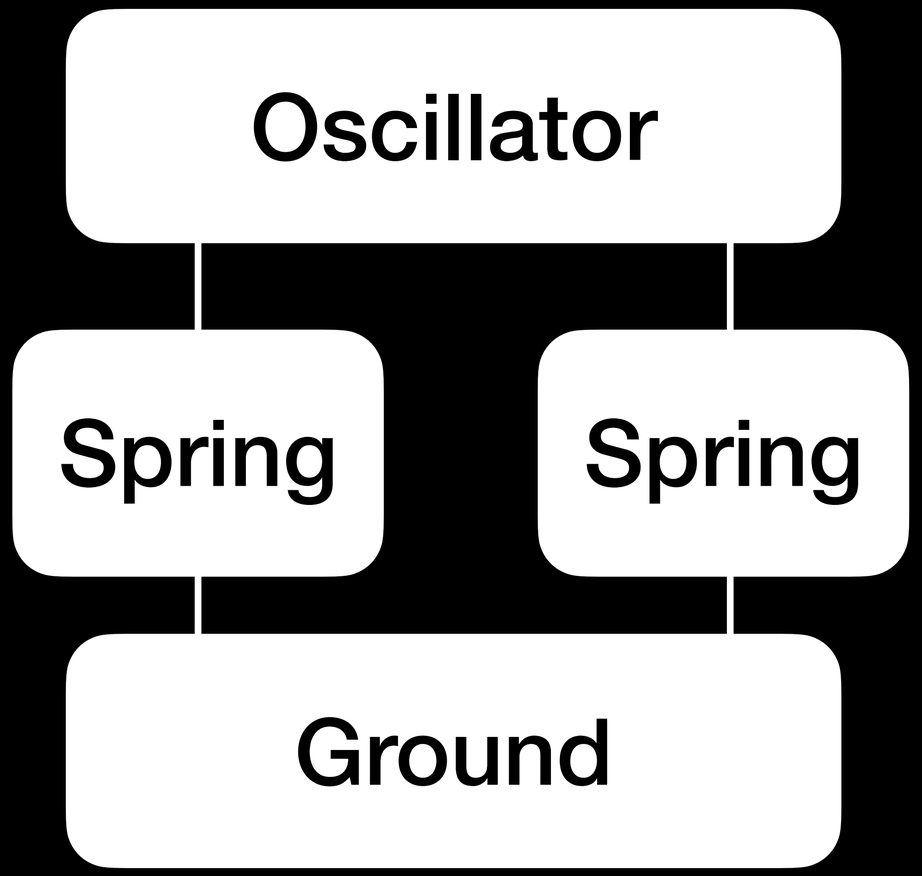

SCL
SDA
AREF
GND
13
12
~11
~10
~9
8
7
~6
~5
DIGITAL - PWM~
L
TX
RX
ARDUINO
UNO R3
RST
EN
JP2

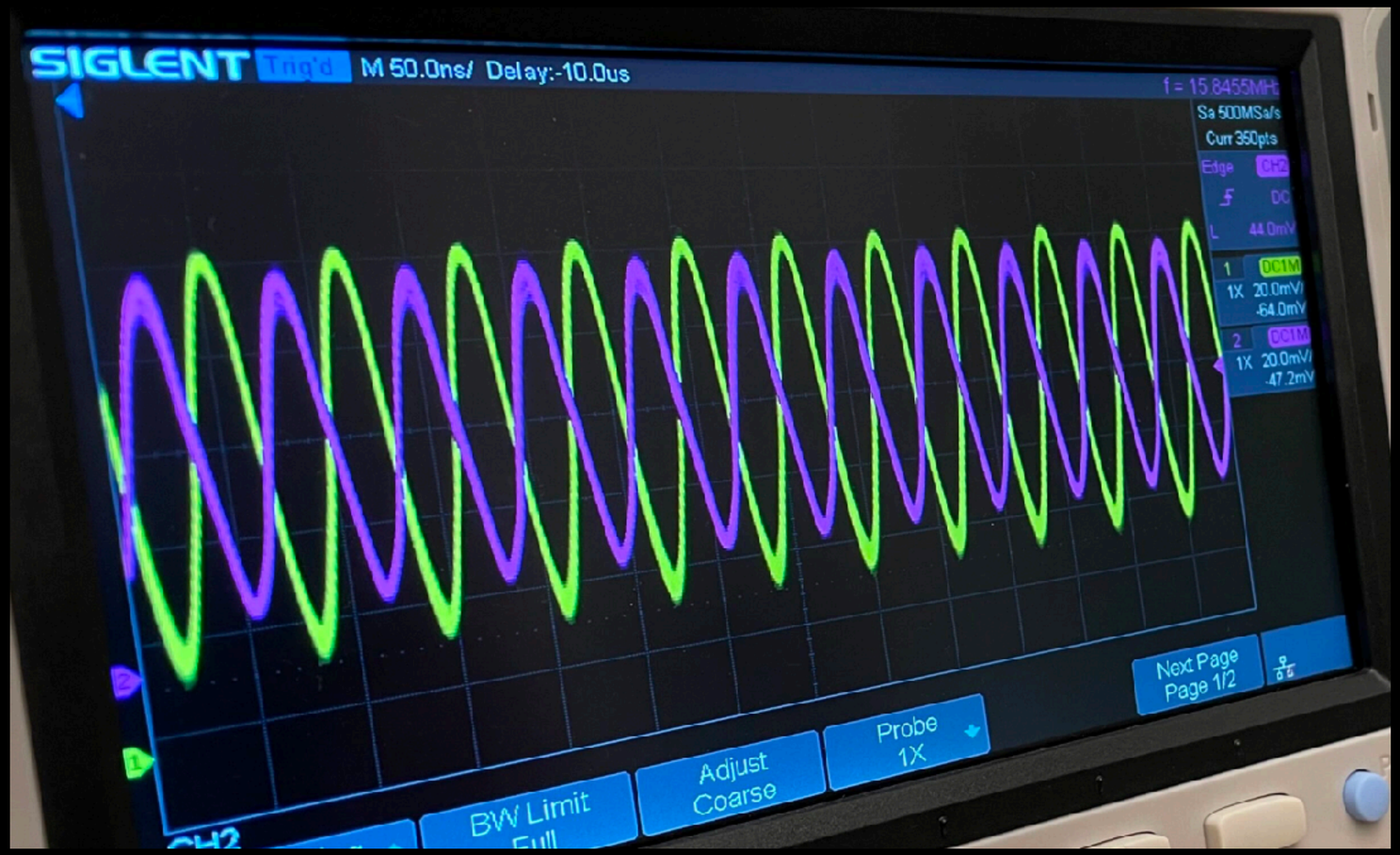


Capacitors

Crystal Oscillator

Clock Glitching





Crystal Oscillator

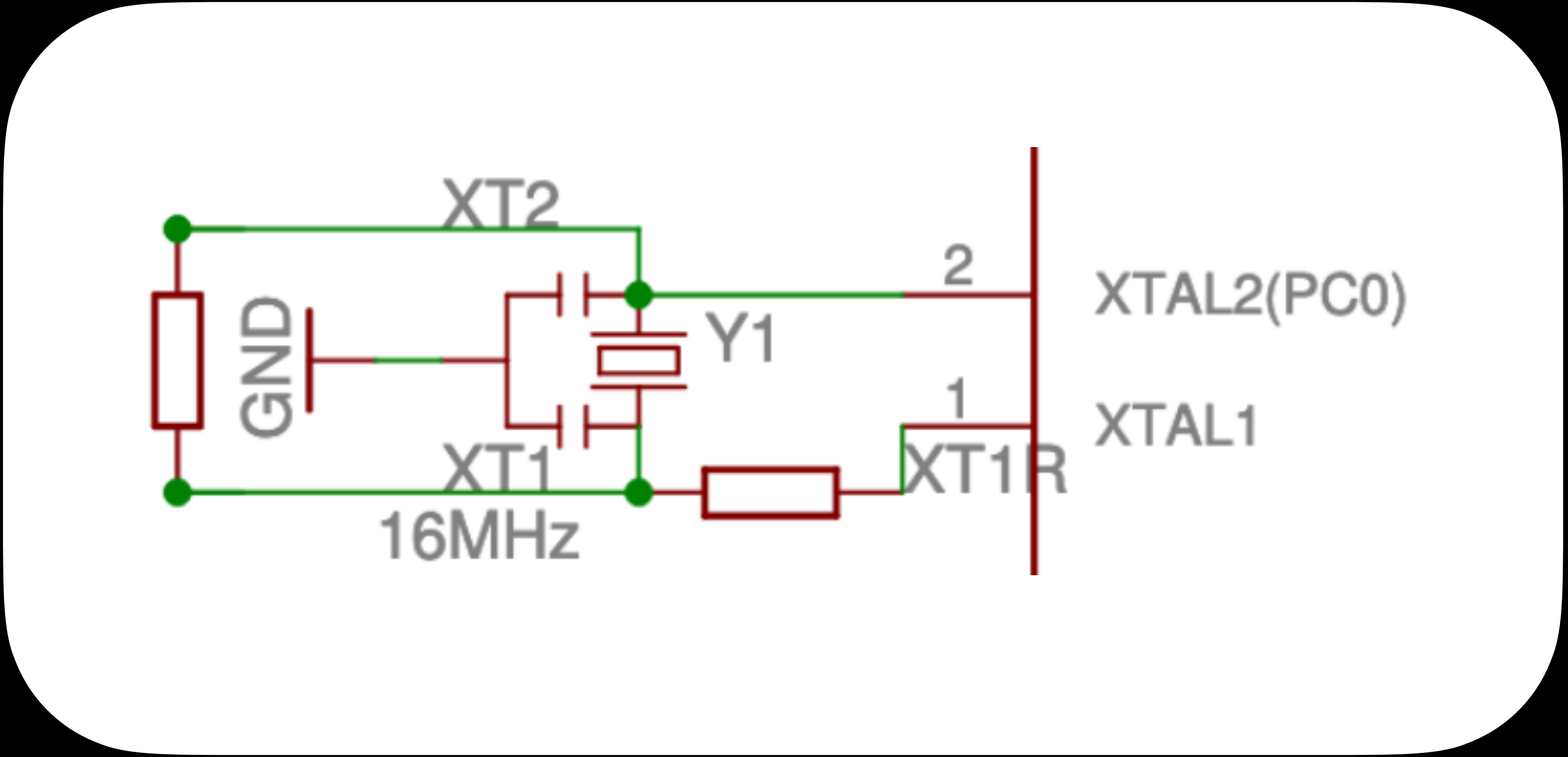


Image: Arduino Uno R3 Reference Design

Crystal Oscillator

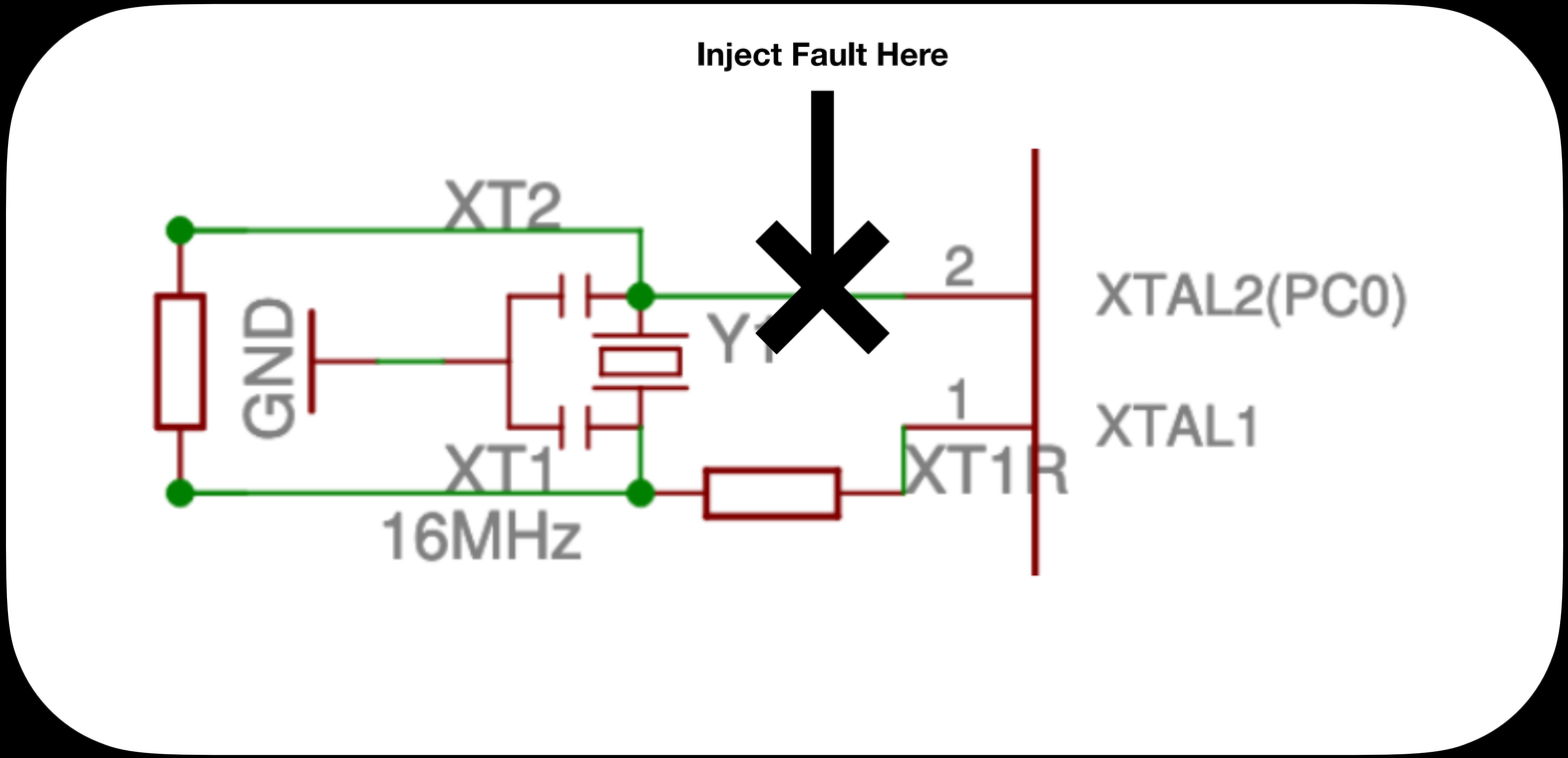
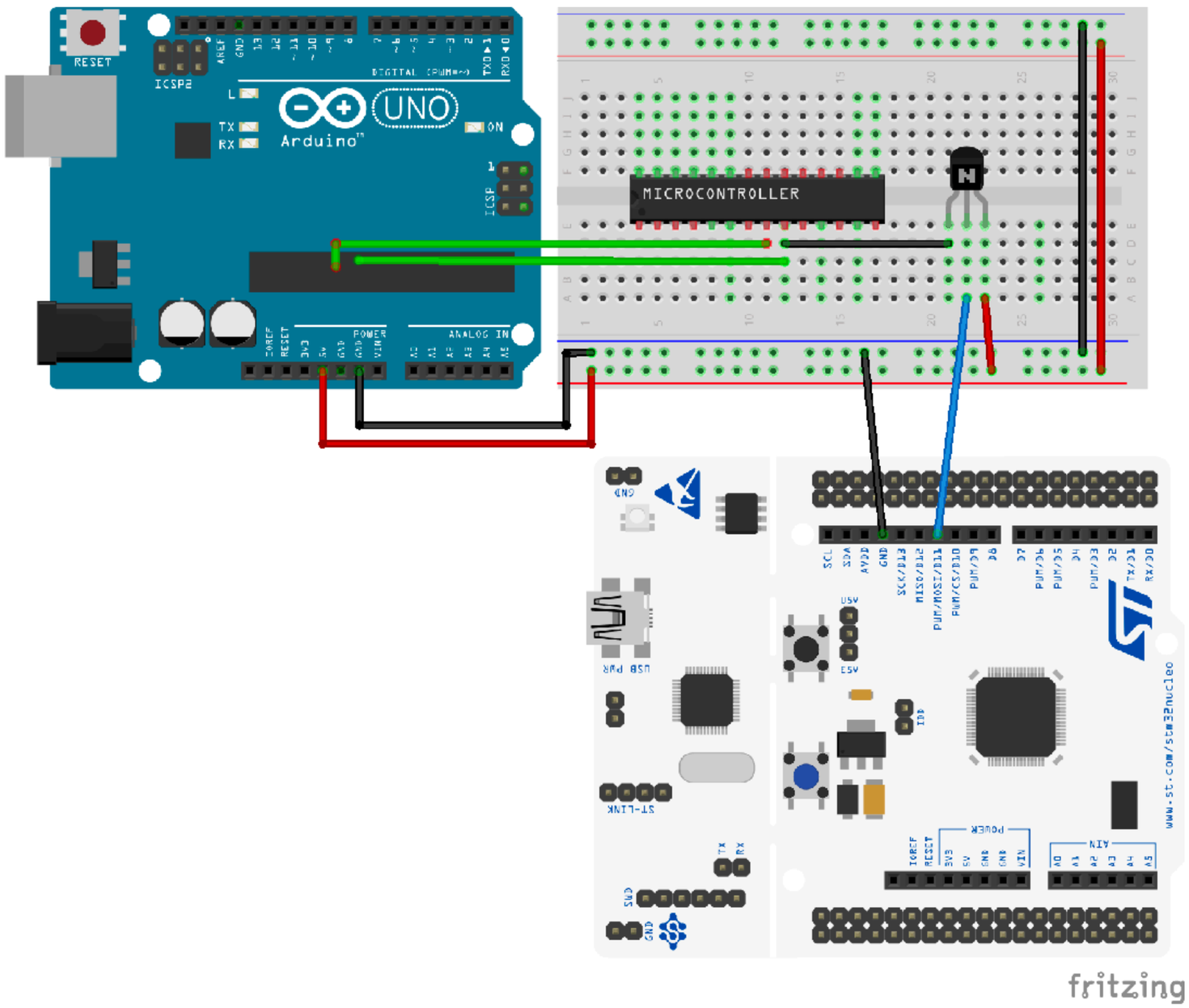


Image: Arduino Uno R3 Reference Design


RESET
ICSP2
UNO
Arduino
MICROCONTROLLER
POWER
ANALOG IN
ICSP
ST-LINK
USB PWR
www.st.com/stm32nucleo
fritzing

Pseudocode

```
void main () {
    int iter = 0;
    while(true) {
        int chksum = compute_checksum();
        print("Locked! %d %d", chksum, iter);
        iter++;
    }
    print("MIT{flag}");
}
```

Demo

Timing Analysis

Spot the Bug

```
bool memcmp (char *buf1, char *buf2, size_t len) {
    for (int i = 0; i < len; i++) {
        if (buf1[i] != buf2[i]) {
            return false;
        }
    }
    return true;
}
```

Spot the Bug

```
bool memcmp (char *buf1, char *buf2, size_t len) {
    for (int i = 0; i < len; i++) {
        if (buf1[i] != buf2[i]) {
            return false;
        }
    }
    return true;
}
```

Fatal Flaw

No Demo:
You will do this in recitation next week!

Coldboot

Static RAM Cell

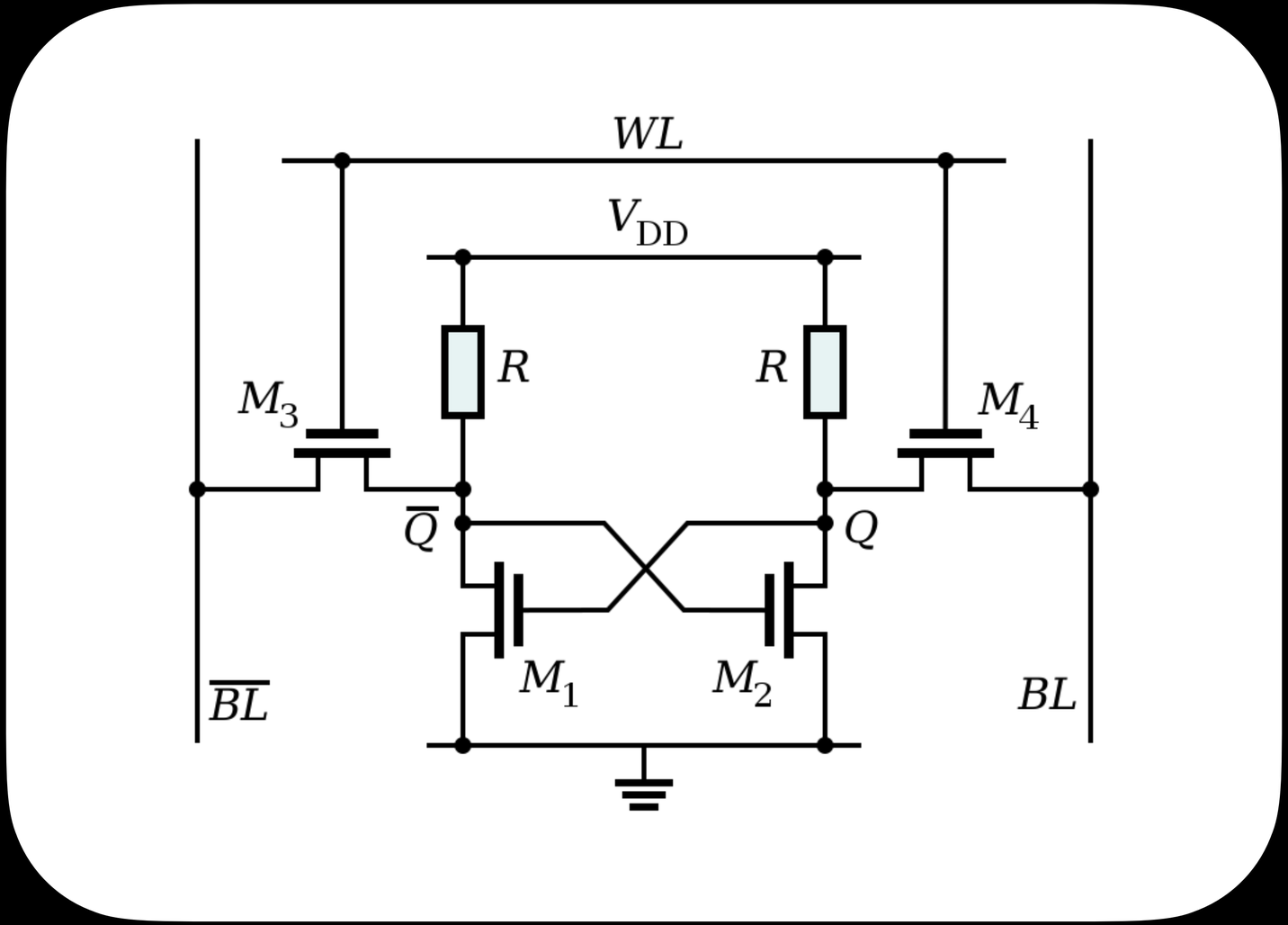
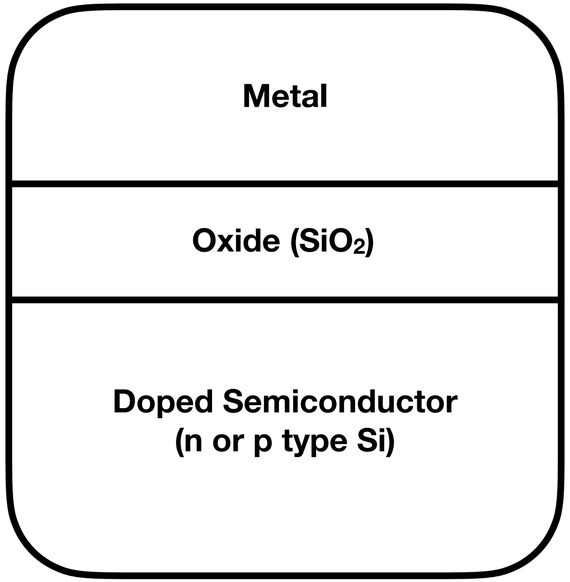
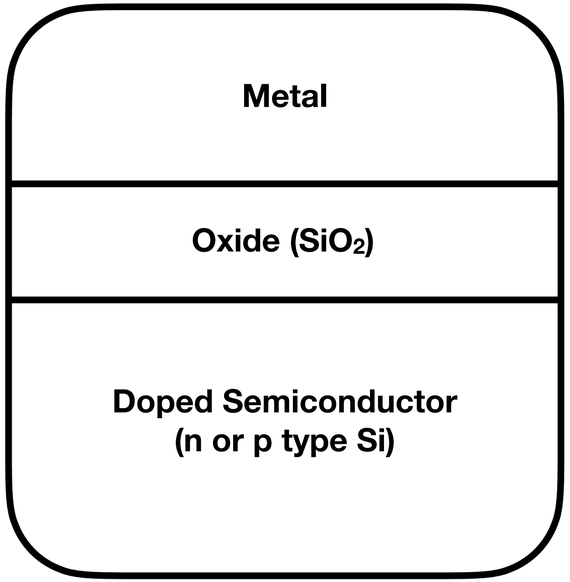


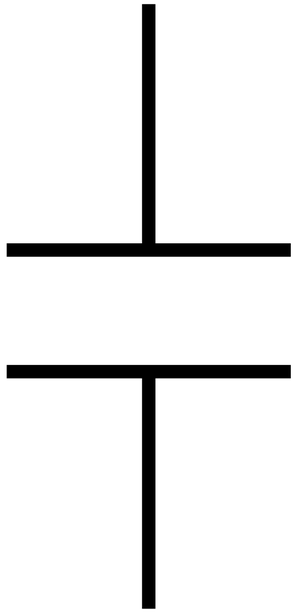
Image: Wikimedia Creative Commons

MOS Capacitor



MOS Capacitor





Demo

Power Analysis

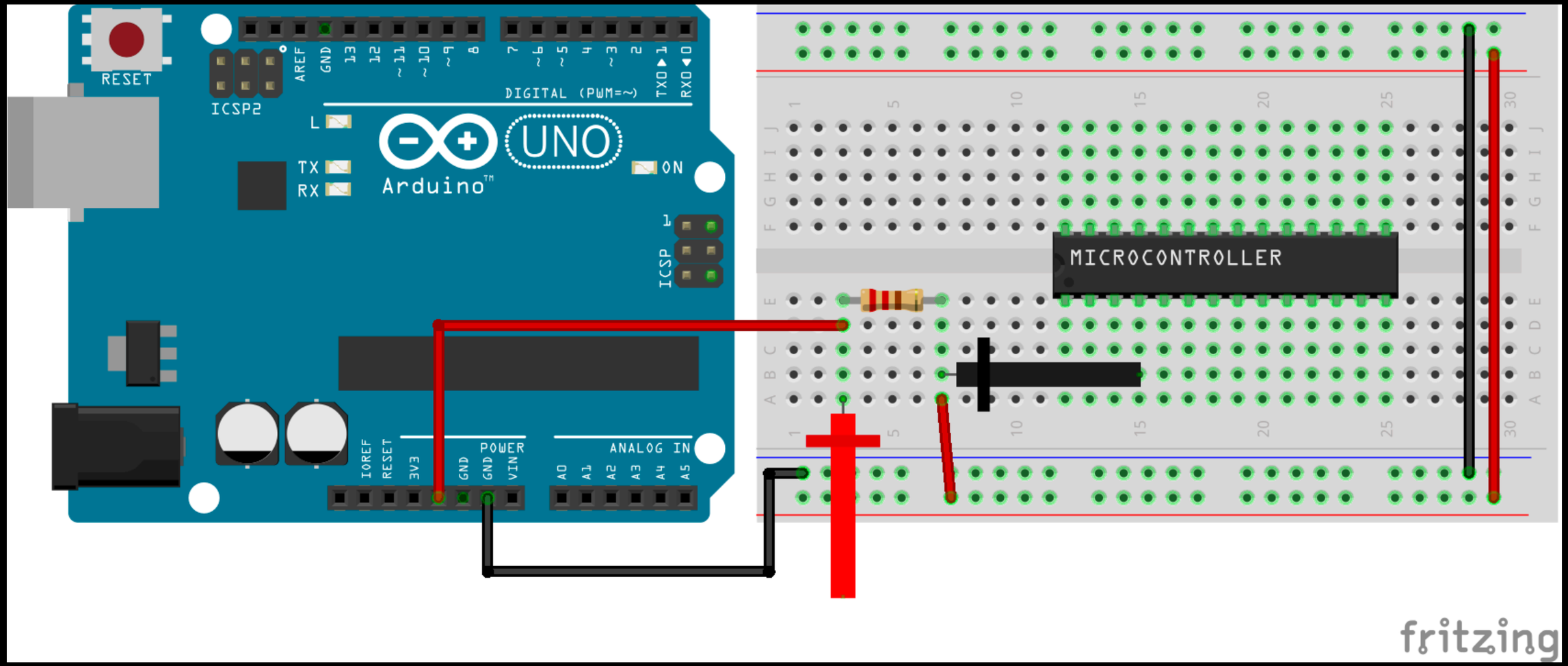
How can you measure current on an oscilloscope?

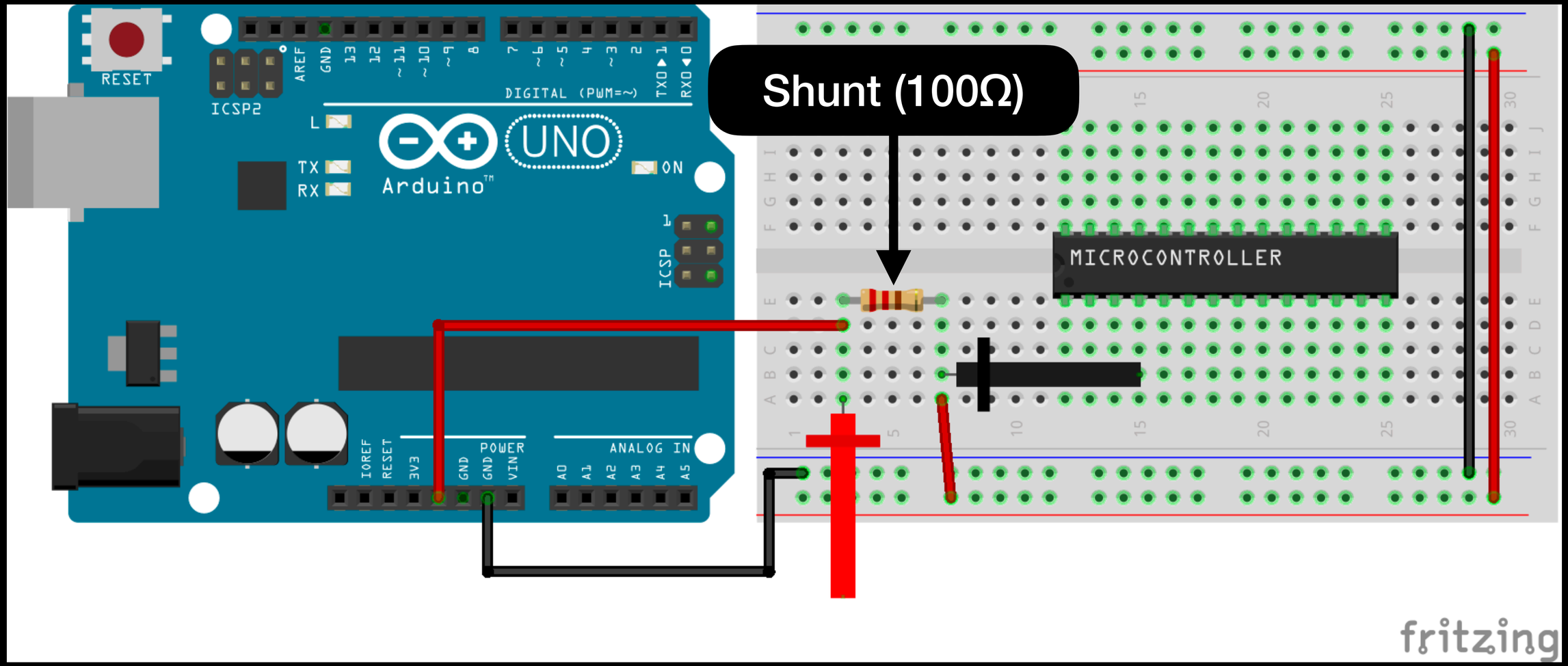
Apply Ohm's Law

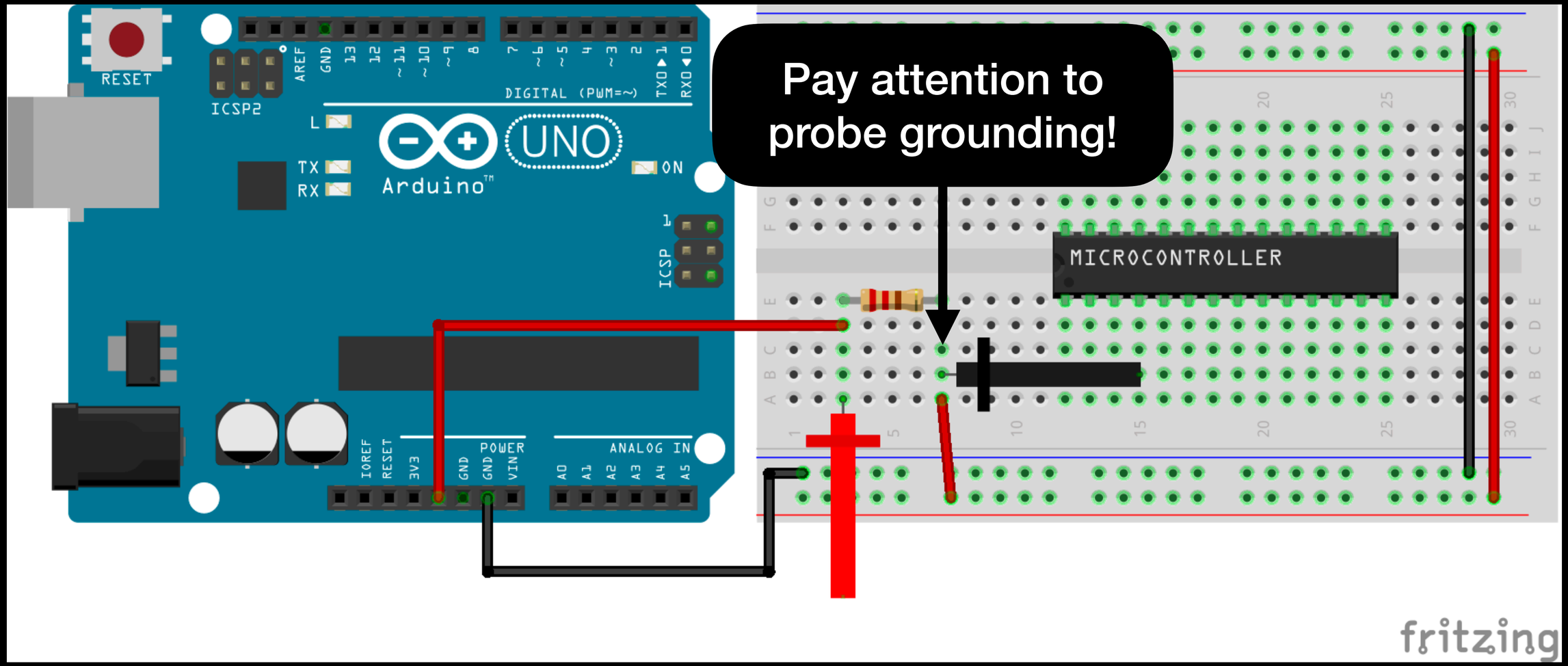
Voltage (V) = Current (I) * Resistance (R)

Or in other words,

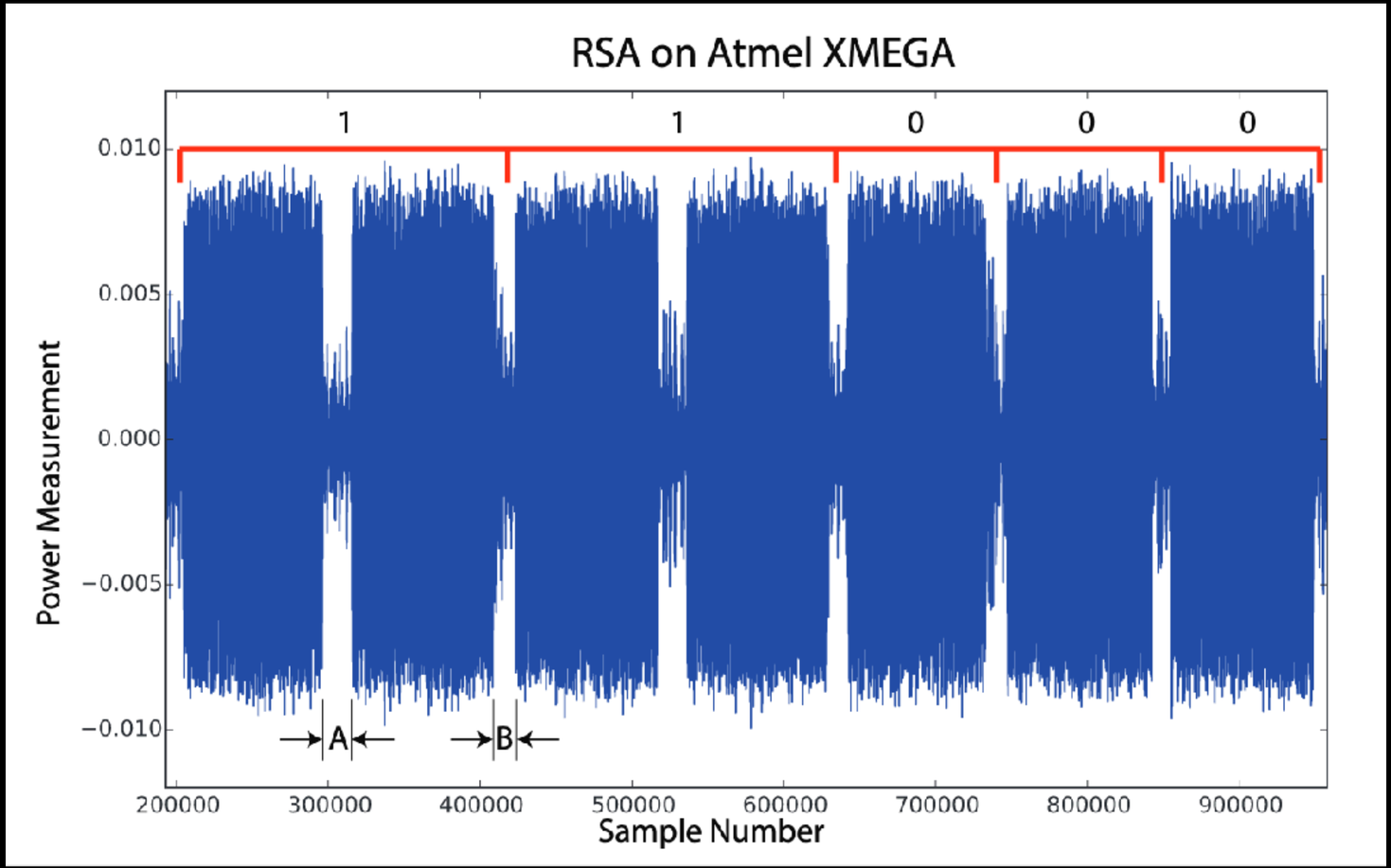
$$I = V / R$$


RESET
ICSP2
AREF
GND
13
12
~11
~10
~9
8
7
~6
~5
4
~3
2
TX0 1
RX0 0
DIGITAL (PWM=~)
L
TX
RX
UNO
Arduino
ON
ICSP
IOREF
RESET
3V3
GND
GND
VIN
POWER
A0
A1
A2
A3
A4
A5
ANALOG IN
MICROCONTROLLER
fritzing


Shunt (100Ω)
MICROCONTROLLER
RESET
ICSP2
AREF
GND
13
12
11
10
9
8
7
6
5
4
3
2
TX0 1
RX0 0
DIGITAL (PWM=~)
L
TX
RX
UNO
Arduino
ON
ICSP
IOREF
RESET
3V3
GND
GND
VIN
POWER
A0
A1
A2
A3
A4
A5
ANALOG IN
fritzing


Pay attention to probe grounding!
RESET
ICSP2
AREF
GND
13
12
~ 11
~ 10
~ 9
8
7
~ 6
~ 5
4
~ 3
2
TX→ 1
RX← 0
DIGITAL (PWM=~)
L
TX
RX
UNO
Arduino
ON
ICSP
MICROCONTROLLER
IOREF
RESET
3V3
GND
GND
VIN
POWER
A0
A1
A2
A3
A4
A5
ANALOG IN
fritzing

Simple Power Analysis

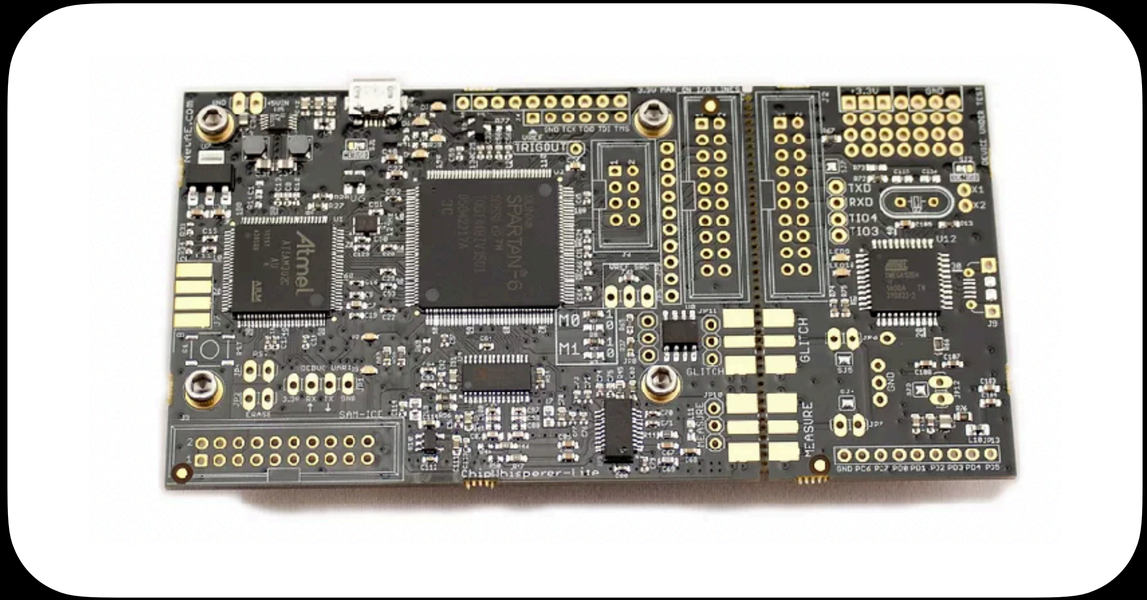


Colin O'Flynn and Greg d'Eon, "I, for one, Welcome Our New Power Analysis Overloads". BlackHat 2018.

Differential Power Analysis

Paul Kocher, Joshua Jaffe, Benjamin Jun

- Statistical analysis of power traces
- Leak the contents of internal device bus



ChipWhisperer-Lite 32-Bit, NewAE Technology Inc.

RSA Modular Exponentiation


```
int rsa_modExp(int b, int e, int m) {
  int product = 1;
  b = b % m;
  while ( e > 0){
    if (e & 1){
      product = modmult(product, b, m);
    }
    b = modmult(b, b, m);

    e >>= 1;
  }
  return product;
}
```

RSA Modular Exponentiation


```
int rsa_modExp(int b, int e, int m) {
  int product = 1;
  b = b % m;
  while ( e > 0){
    if (e & 1){
      product = modmult(product, b, m);
    }
    b = modmult(b, b, m);

    e >>= 1;
  }
  return product;
}
```

RSA Modular Exponentiation


```
int rsa_modExp(int b, int e, int m) {
  int product = 1;
  b = b % m;
  while ( e > 0){
    if (e & 1){
      product = modmult(product, b, m);
    }
    b = modmult(b, b, m);

    e >>= 1;
  }
  return product;
}
```

RSA Modular Exponentiation

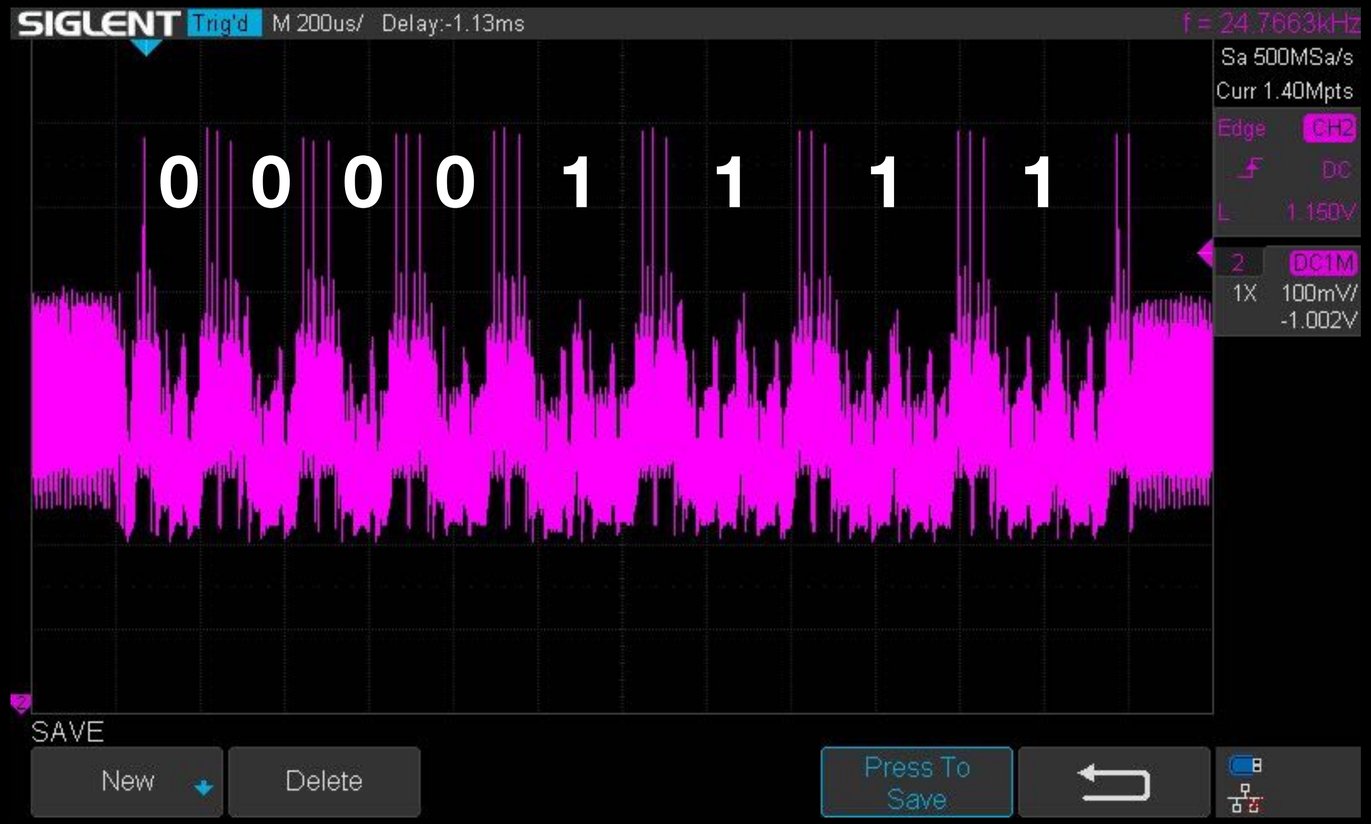
1 call to `modmult`

```
int rsa_modExp(int b, int e, int m) {
  int product = 1;
  b = b % m;
  while ( e > 0){
    if (e & 1){
      product = modmult(product, b, m);
    }
    b = modmult(b, b, m);

    e >>= 1;
  }
  return product;
}
```

RSA Modular Exponentiation


```
int rsa_modExp(int b, int e, int m) {
  int product = 1;
  b = b % m;
  while ( e > 0){
    if (e & 1){
      product = modmult(product, b, m);
    }
    b = modmult(b, b, m);

    e >>= 1;
  }
  return product;
}
```

RSA Modular Exponentiation

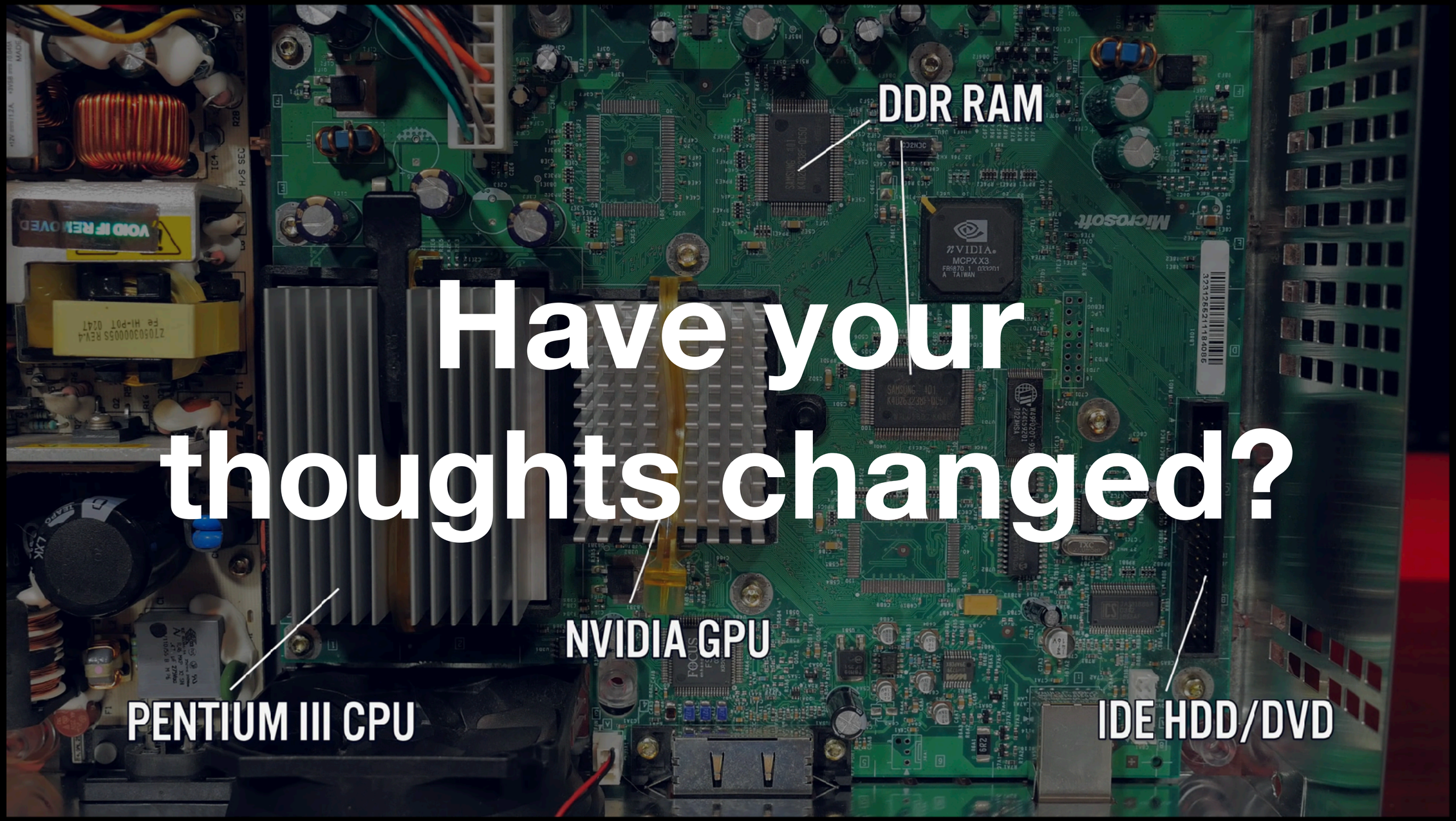



```
int rsa_modExp(int b, int e, int m) {
  int product = 1;
  b = b % m;
  while ( e > 0){
    if (e & 1){
      product = modmult(product, b, m);
    }
    b = modmult(b, b, m);

    e >>= 1;
  }
  return product;
}
```

e = 0xf0

Demo

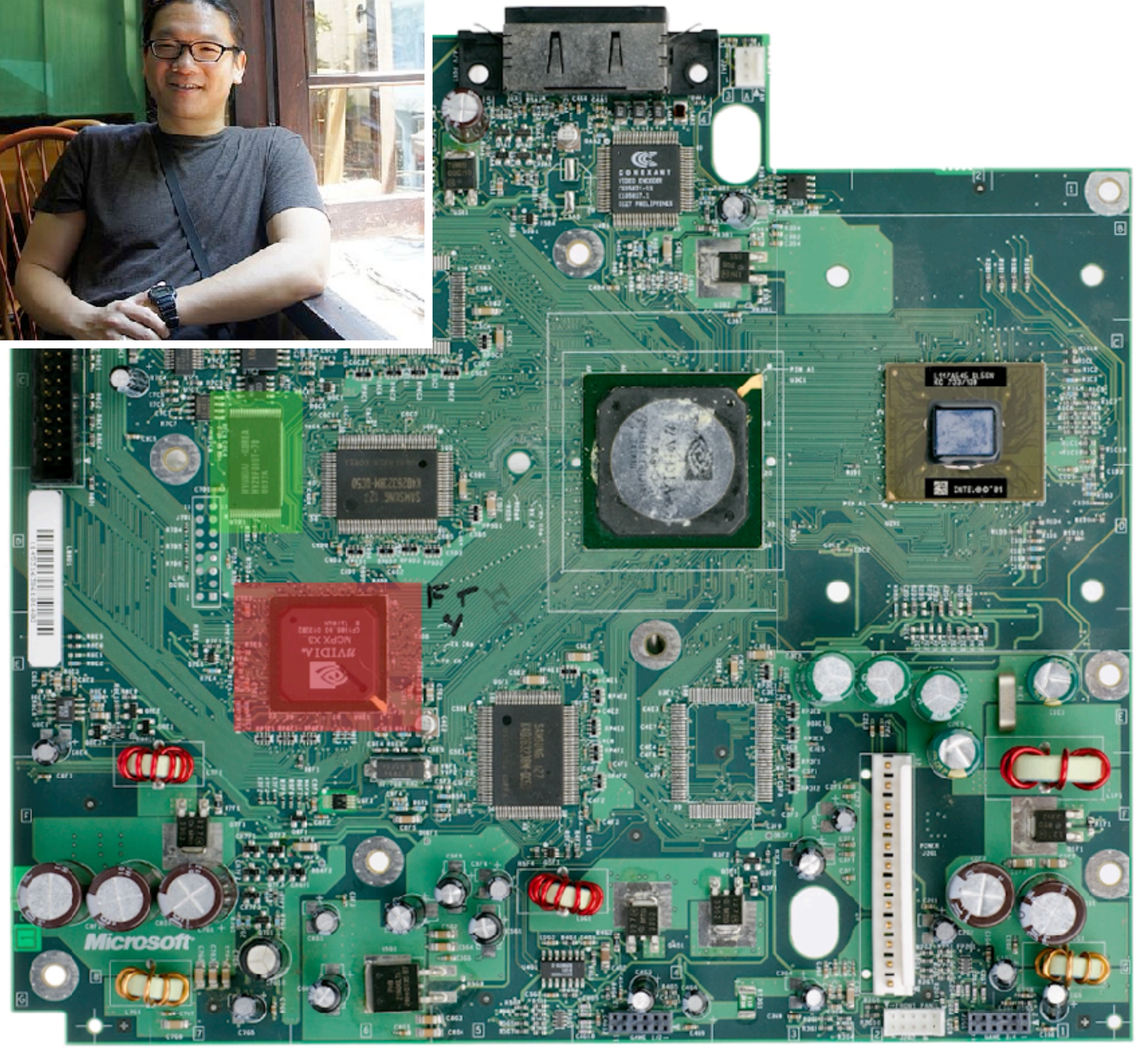
Back to the Xbox...



Have your thoughts changed?

Image: Modern Vintage Gamer (YouTube)

bunnie



- "SECRET ROM" STORED IN MCPX
- FLASH DECRYPTION KEY (RC4) STORED IN "SECRET ROM"
- DATA BUS "SNIFFER" BUILT BETWEEN FLASH AND MCPX

DECRYPTION KEY DISCOVERED, FLASH KERNEL (BIOS) DECRYPTED AND PATCHED FOR UNSIGNED CODE

Image: Modern Vintage Gamer (YouTube)

What attackers are willing to do (Kamikaze Hack)

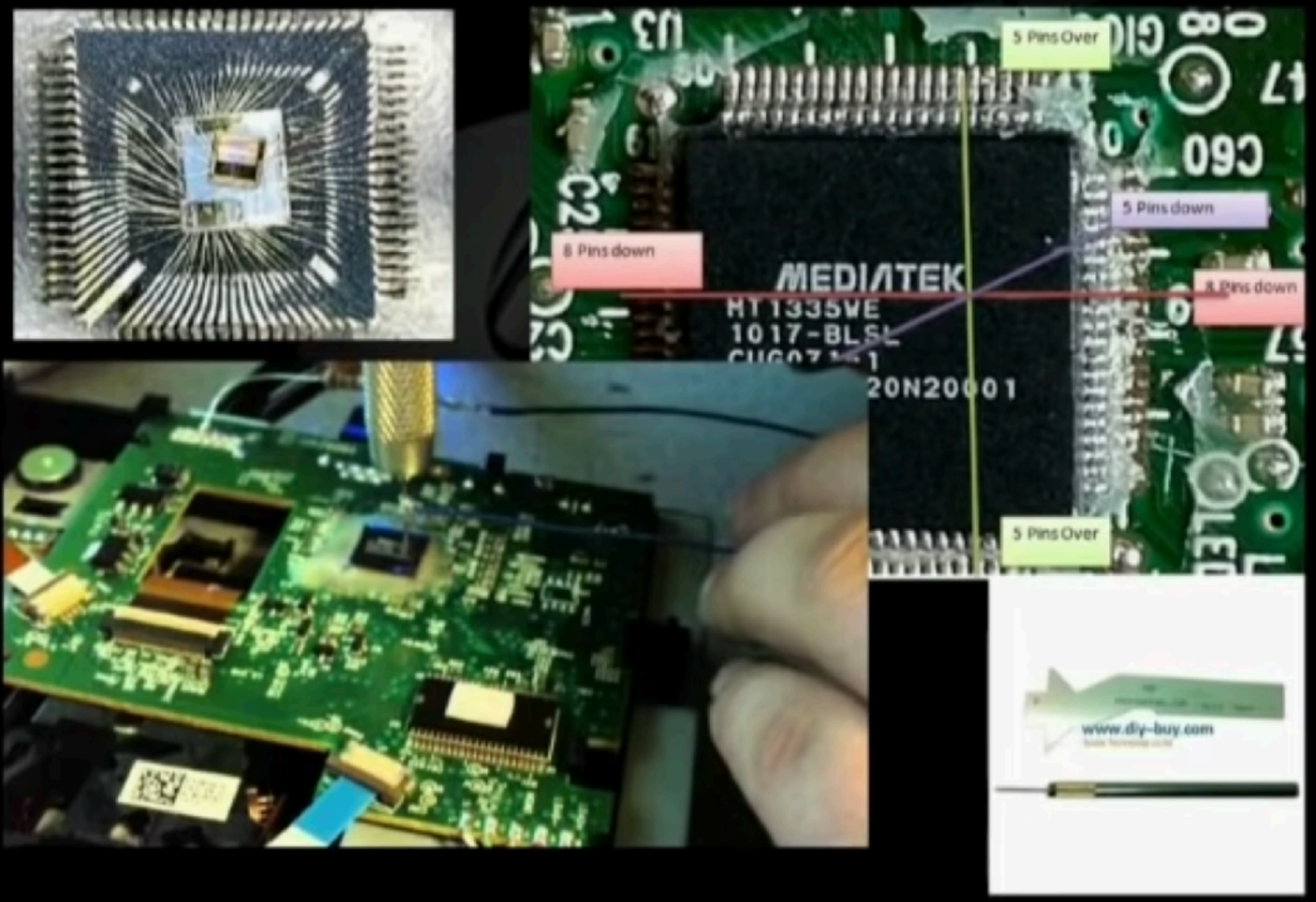


Image: Microsoft

Xbox 360 Reset Glitch Hack (RGH)

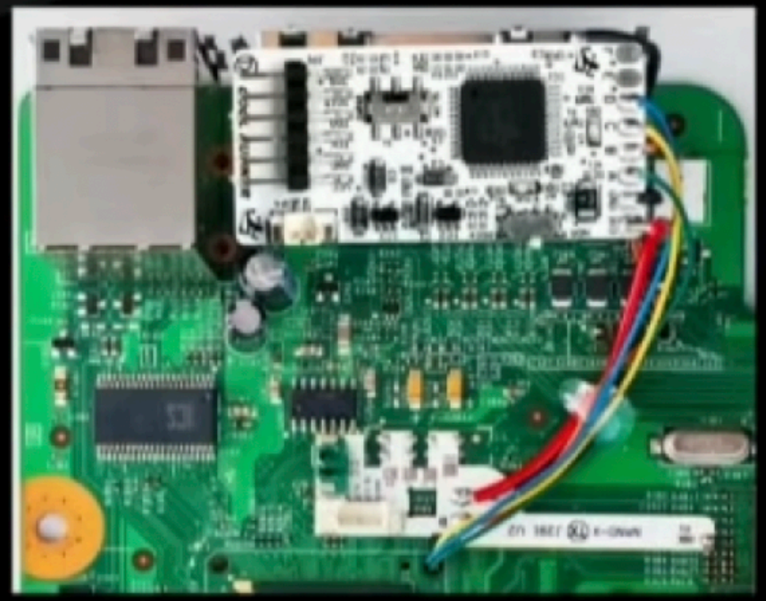


Image: Microsoft

Xbox One Security Architecture

Confidentiality

Plaintext of games and secret keys **never** leave the CPU die

Integrity

Attest software is not compromised before connecting to Xbox Live

Xbox One Security Architecture

Attacker == user

- Any bus / external device considered compromised (flash, HDD, DRAM)
- PCIe, SATA, USB, DRAM bus, motherboard fabric can be intercepted
- Can only trust CPU Si itself

Use a custom chip!

- Encrypt all busses and DRAM contents
- Custom on-die crypto registers hold keys
- Build a shared key between CPU and optical disk drive
- Reduce trusted computing base (TCB) by moving security critical code to a trusted minimal hypervisor
- Bringup uses secure Boot ROM to sign future stages

Takeaways

- Physical attacks pose a new threat model (customer may also be the attacker!)
- Cannot trust anything off-chip
- We can classify attacks based on costs and invasiveness
    - Some attacks are quite cheap...
- Defense in depth (no single point of failure), tradeoff between security and performance
    - Just need to ensure physical attacks aren't easy enough to be worth an attacker's time