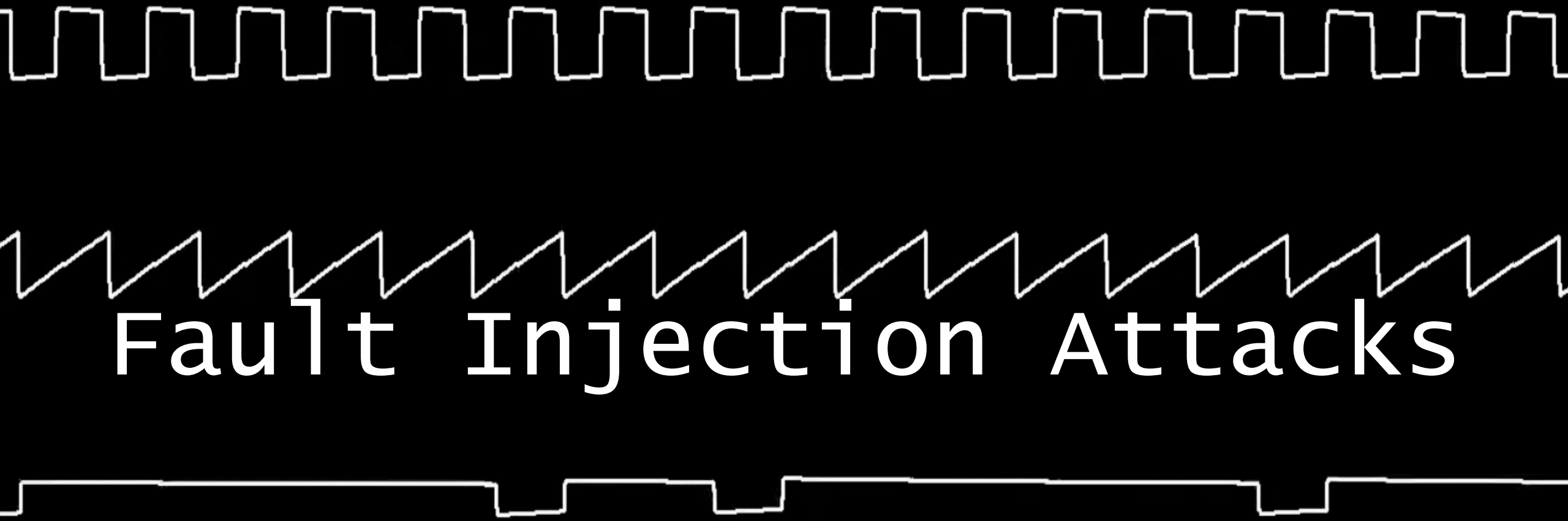


Fault Injection Attacks

Julio Della Flora

Sobre / Julio Della Flora

Especialização em Docência para o Ensino Superior (2017).

Mestrado em Ciência da Informação (2015).

Especialização em Redes de Computadores e Segurança de Dados (2012).

Bacharelado em Ciência da Computação (2010).

Analista de Segurança da Informação na Conviso Application Security, 2018 – Atual.

Coordenador da Pós-Graduação no Centro de Inovação Vincit, 2017 – Atual.

Hardware Fault Injection?

O objetivo desse grupo de ataques é:

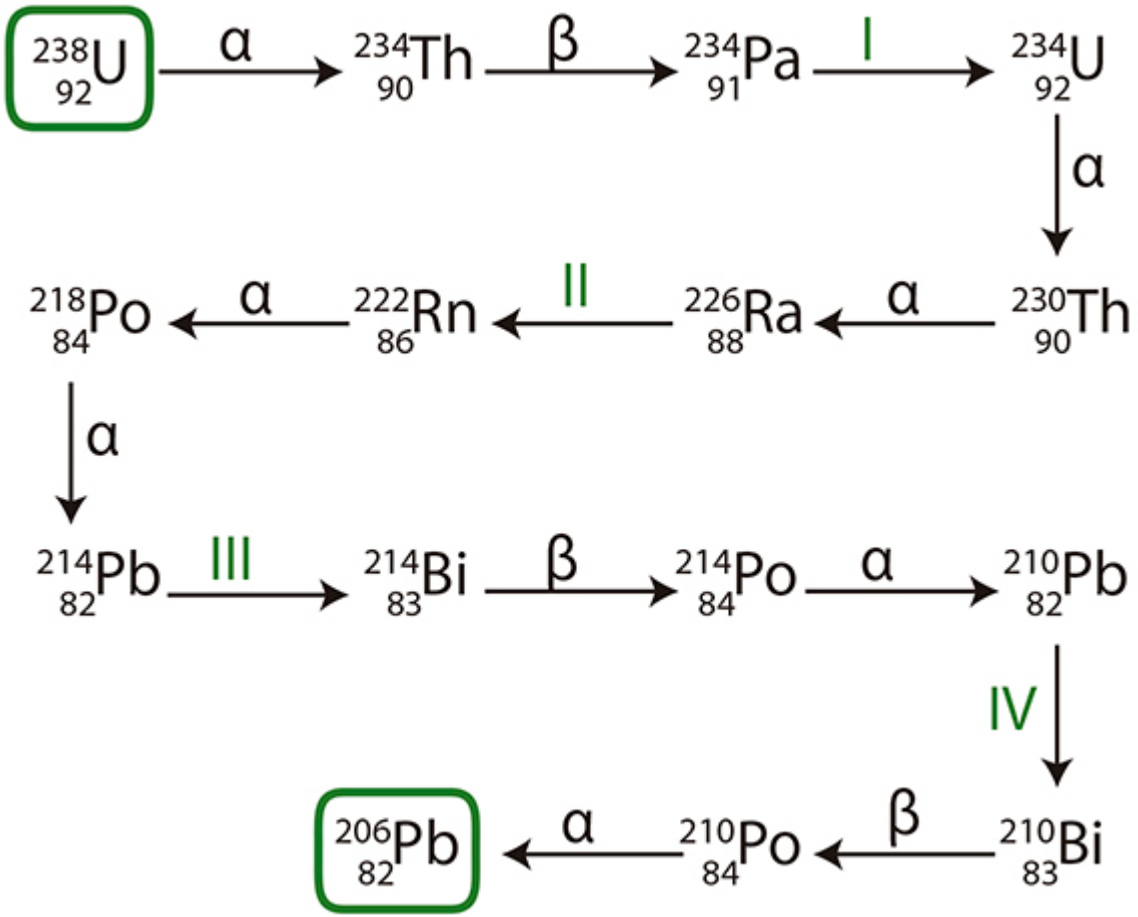
“Introduzir falhas no alvo buscando alterações em seu comportamento padrão, essas falhas são induzidas através da manipulação de condições ambientais em um micro controlador e/ou demais componentes eletrônicos presentes no alvo.”

Um Pouco de História

Os efeitos da indução de falhas em sistemas eletrônicos vêm sendo estudadas desde os anos 1970.

...quando partículas radioativas produzidas por elementos presentes no encapsulamento de chips induziram falhas em seus funcionamentos.

Um Pouco de Física / Química



Elementos como Urânio-235, Urânio-238 e Tório-230 presentes no encapsulamento dos chips decaíram para Chumbo-206 resultando na liberação de partículas Alfa. Essas partículas produziam carga em áreas sensíveis do chip causando a modificação de bits.

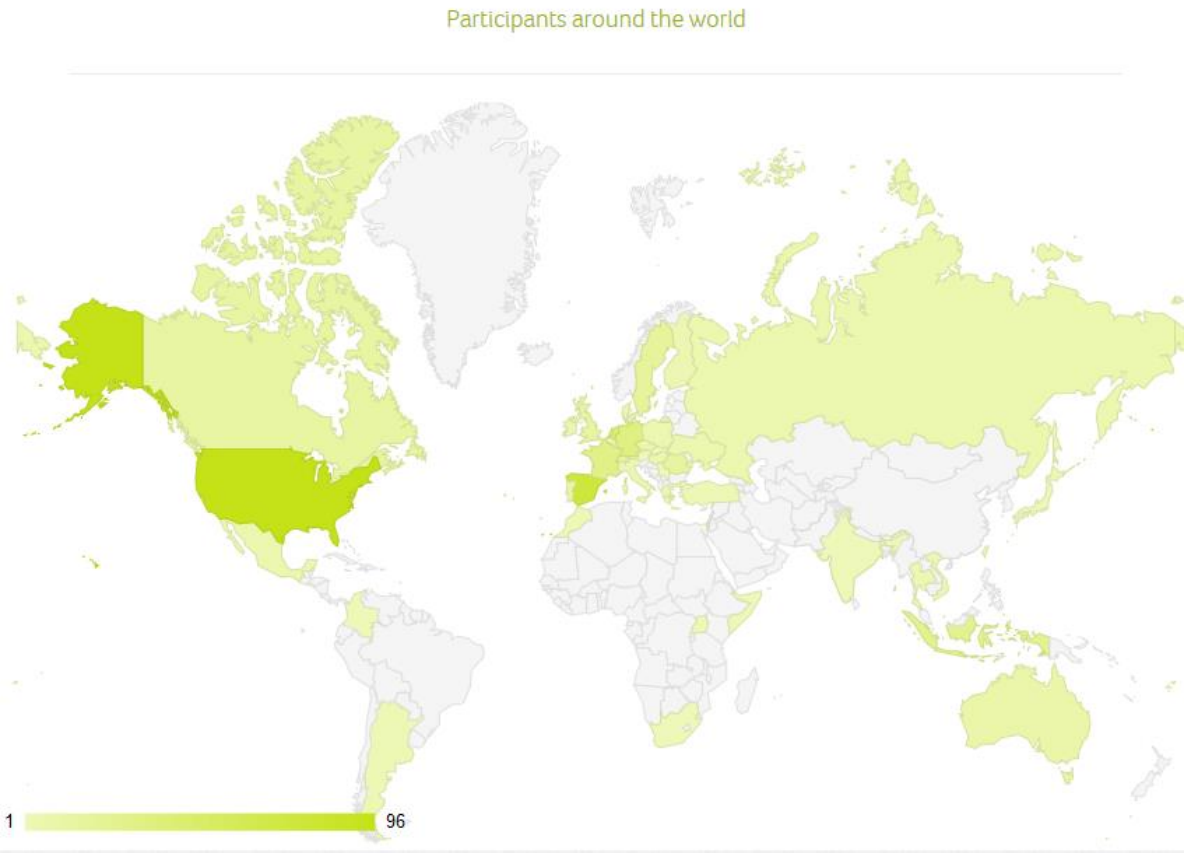
Apenas duas ou três partes por milhão já eram capazes de afetar o comportamento dos sistemas eletrônicos.

Um Pouco de História

Pesquisas com raios cósmicos em semicondutores também foram conduzidas a partir dessa época, apesar desse tipo de emanação ser muito fraca dentro de nossa atmosfera ela era capaz de afetar equipamentos fora do nosso planeta, se tornando um ponto de interesse para organizações como NASA e Boeing.

https://www.inovacaotecnologica.com.br/noticias/noticia.php?artigo=raios-cosmicos-derrubaram-phobos-grunt&id=020175120131

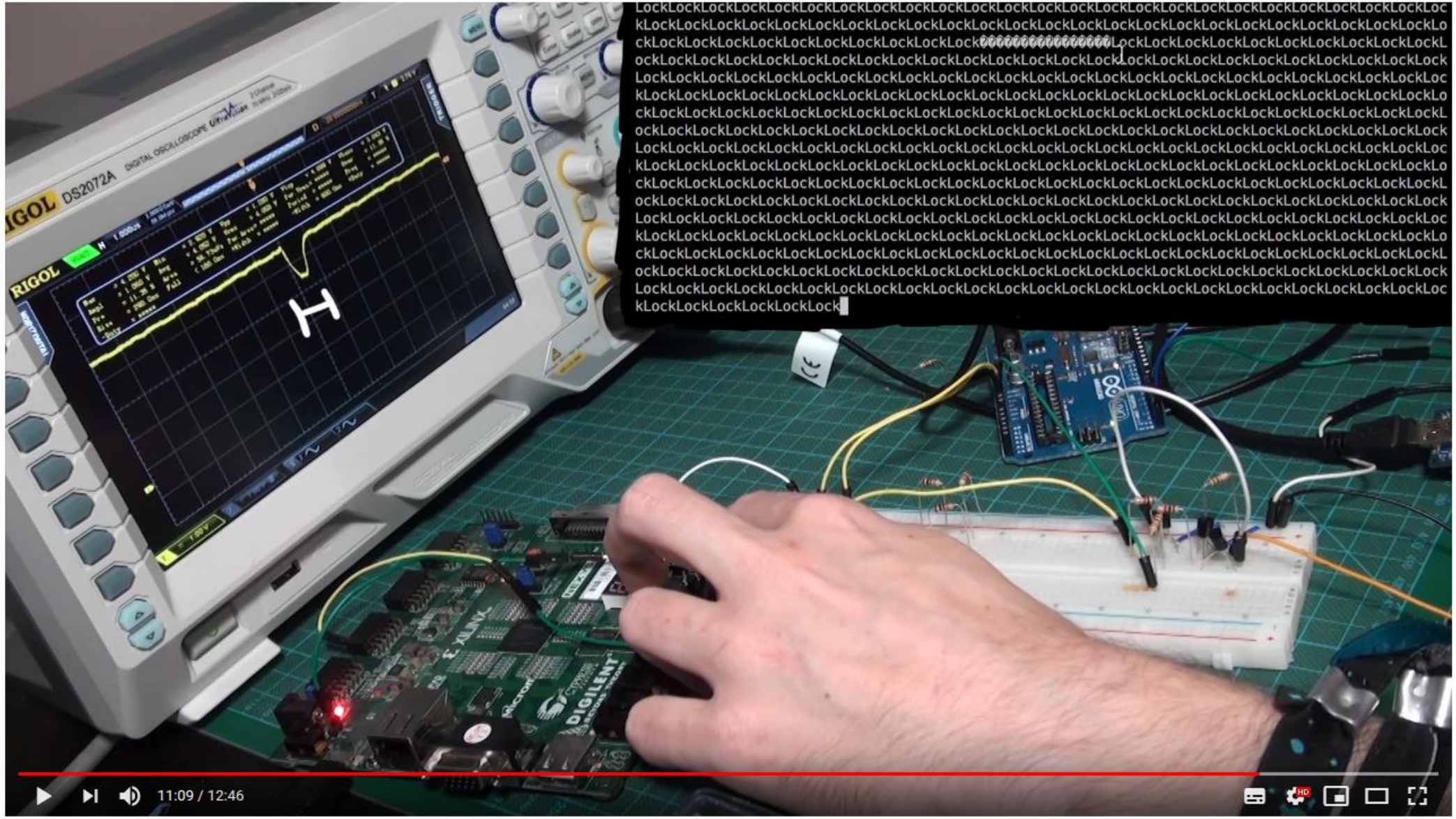
Riscure Hack Me 2... um CTF interessante...



Nenhum time brasileiro cadastrado.

Glitch Attack – Fiesta (FI 100)

Como quebrar um loop infinito em uma placa Arduino?



Hardware Power Glitch Attack - rhme2 Fiesta (FI 100)

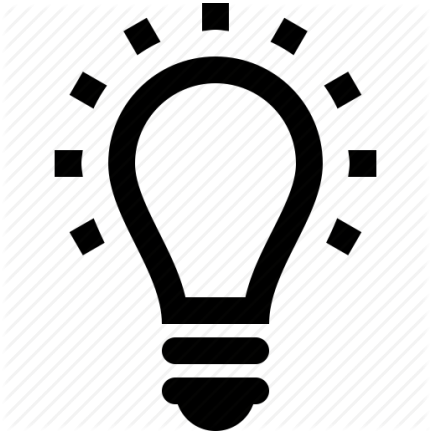
15.131 visualizações

623 4 COMPARTILHAR

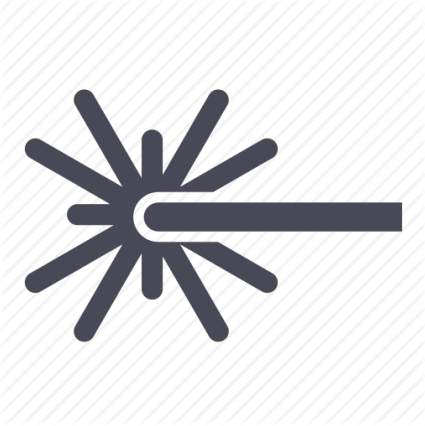
LiveOverflow
Publicado em 16 de jun de 2017

DOWNLOAD AS: ▼ INSCRITO 146 MIL

Classificando Injeções de Falha

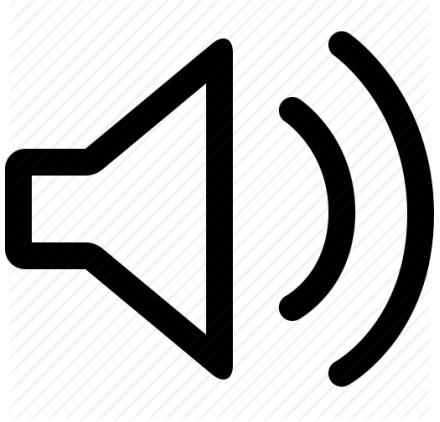


Luz Branca



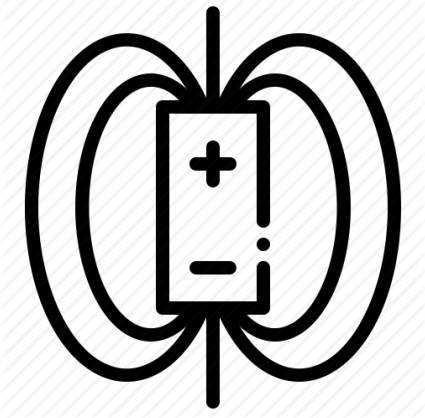
Laser

Clock



Ultrassom

Temperatura

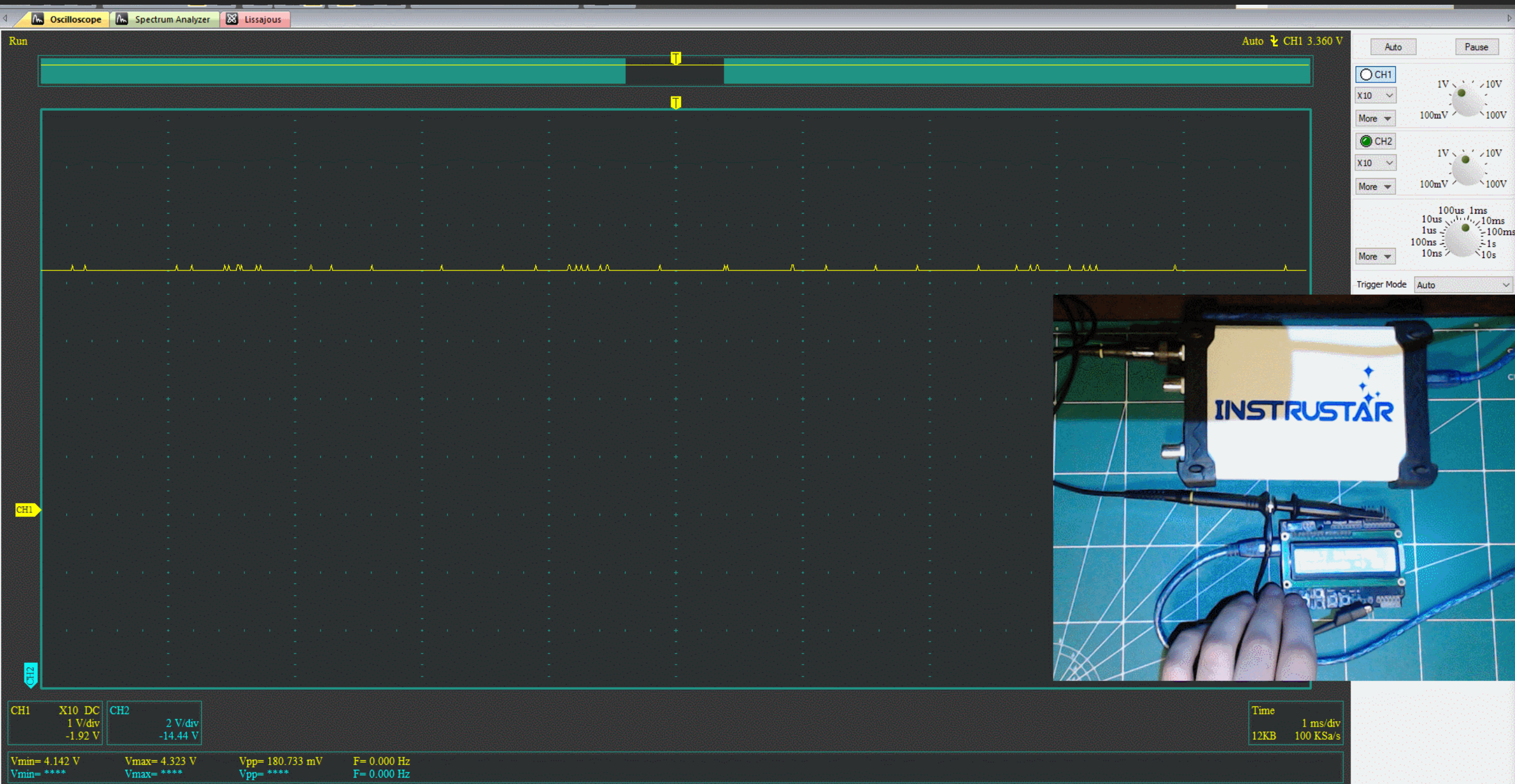


Eletromagnetismo

Tensão

FONTE: The Sorcerers Apprentice Guide to Fault Attacks. – Bar-El et al., 2004

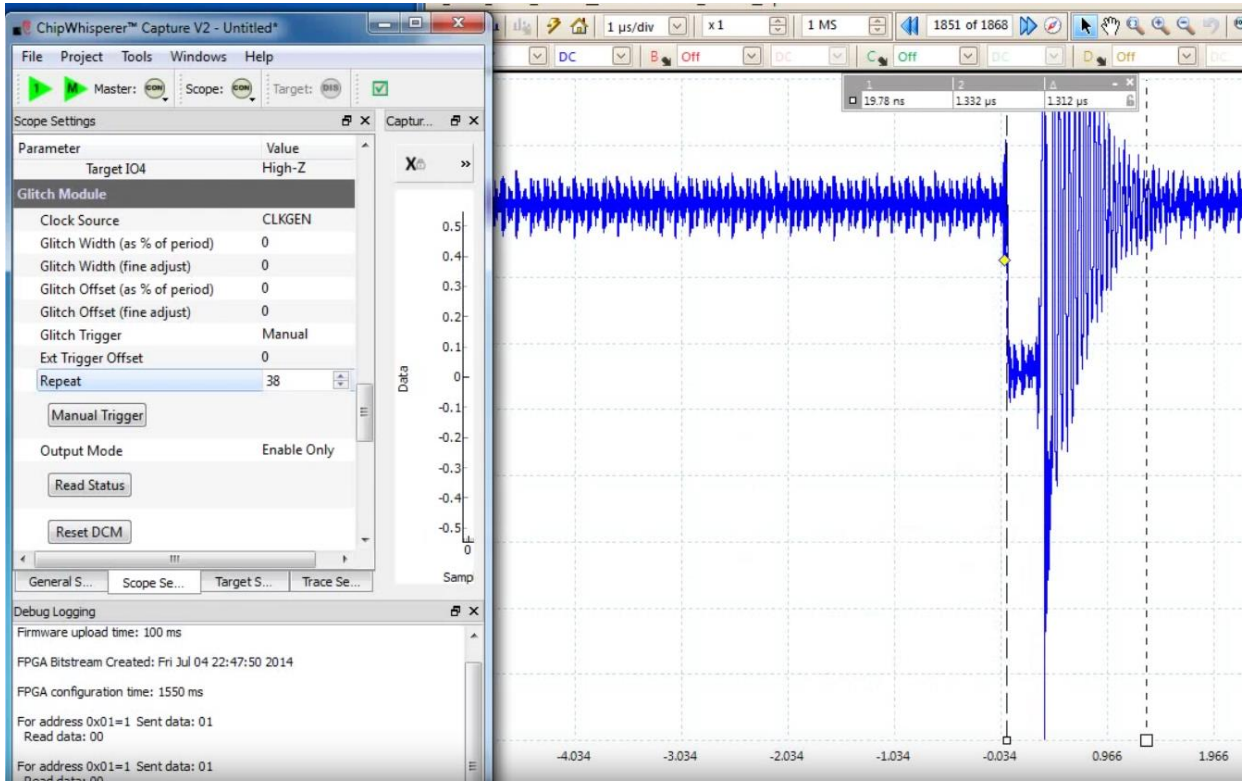
Voltage Fault Injection / Power Glitch



Voltage Fault Injection

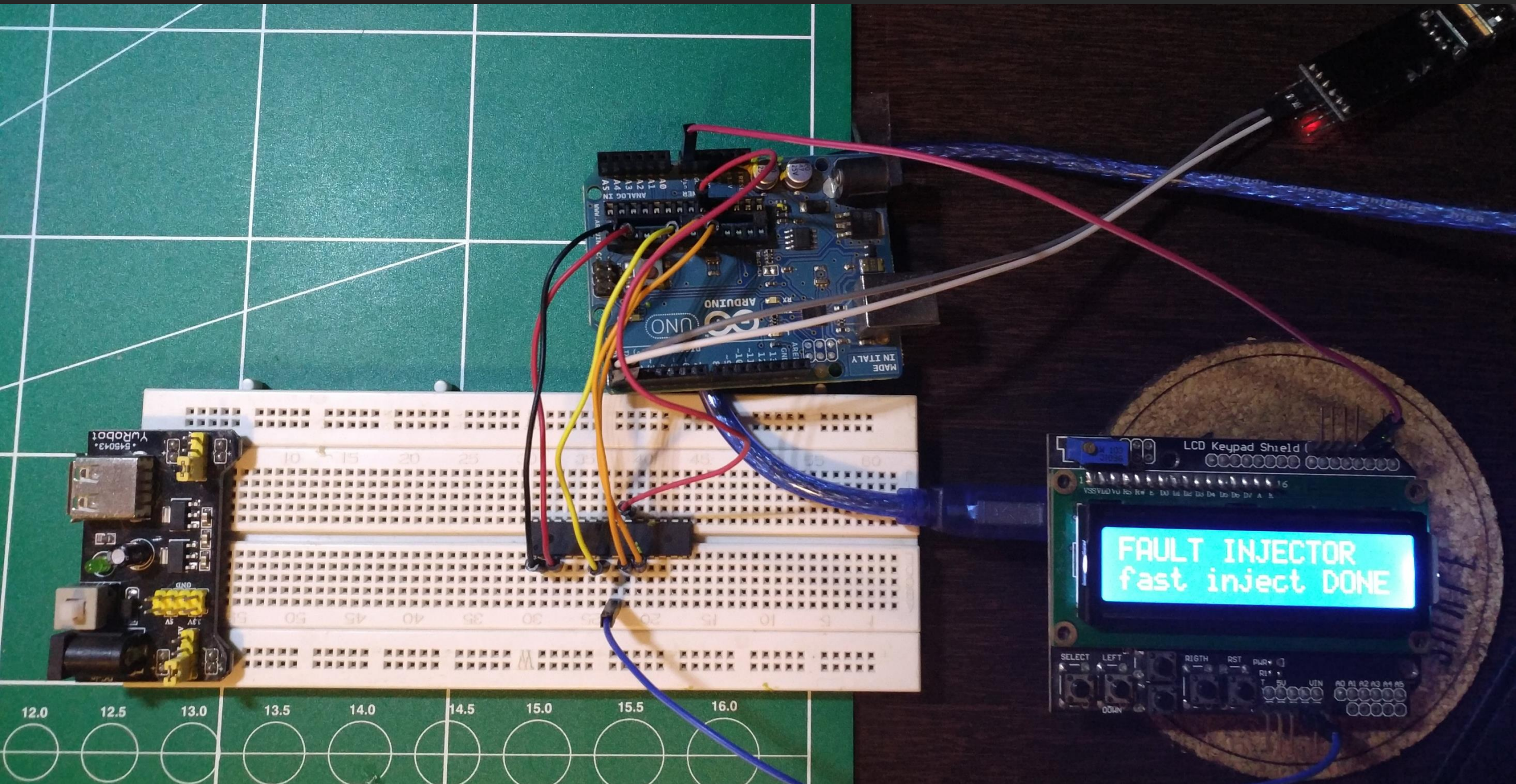
As variações no fornecimento de tensão podem causar falha na interpretação de instruções ou mesmo a não interpretação de instruções por parte de um micro controlador.

Quedas ou sobrecargas de tensão podem ser induzidas para que o chip deixe de interpretar uma instrução, ou interprete de maneira errônea essa mesma instrução. É comum simular quedas de tensão (Volts) de poucos nano segundos buscando manter o funcionamento de apenas algumas partes de um micro controlador.



FONTE: https://hackaday.io/project/956-chipwhisperer-security-research/log/5120-glitching-a-linux-target

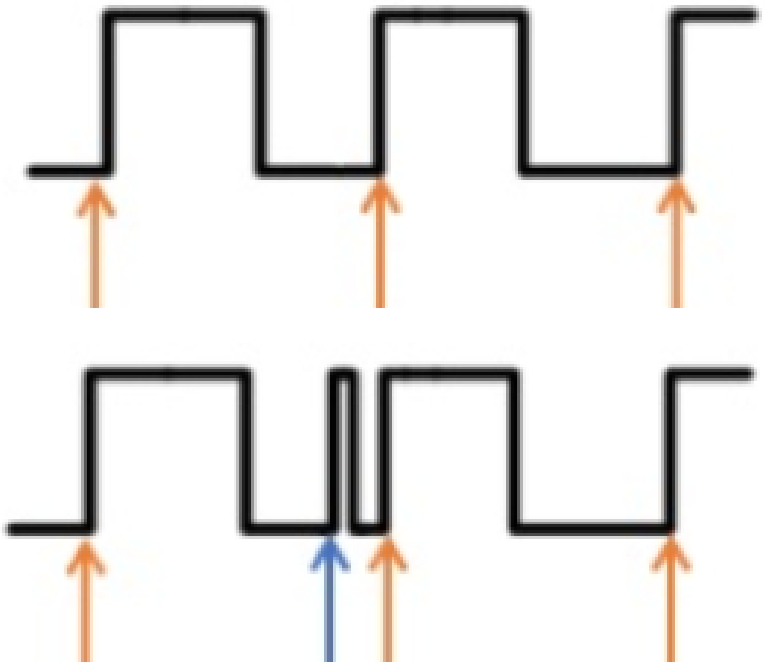
Eu tentei...


LCD Keypad Shield
FAULT INJECTOR
fast inject DONE
SELECT
LEFT
RIGTH
RST
DOWN
ARDUINO
UNO
MADE IN ITALY

Clock Fault Injection

Variações do ataque baseando-se em *clock* podem causar má interpretação ou falta da instrução.

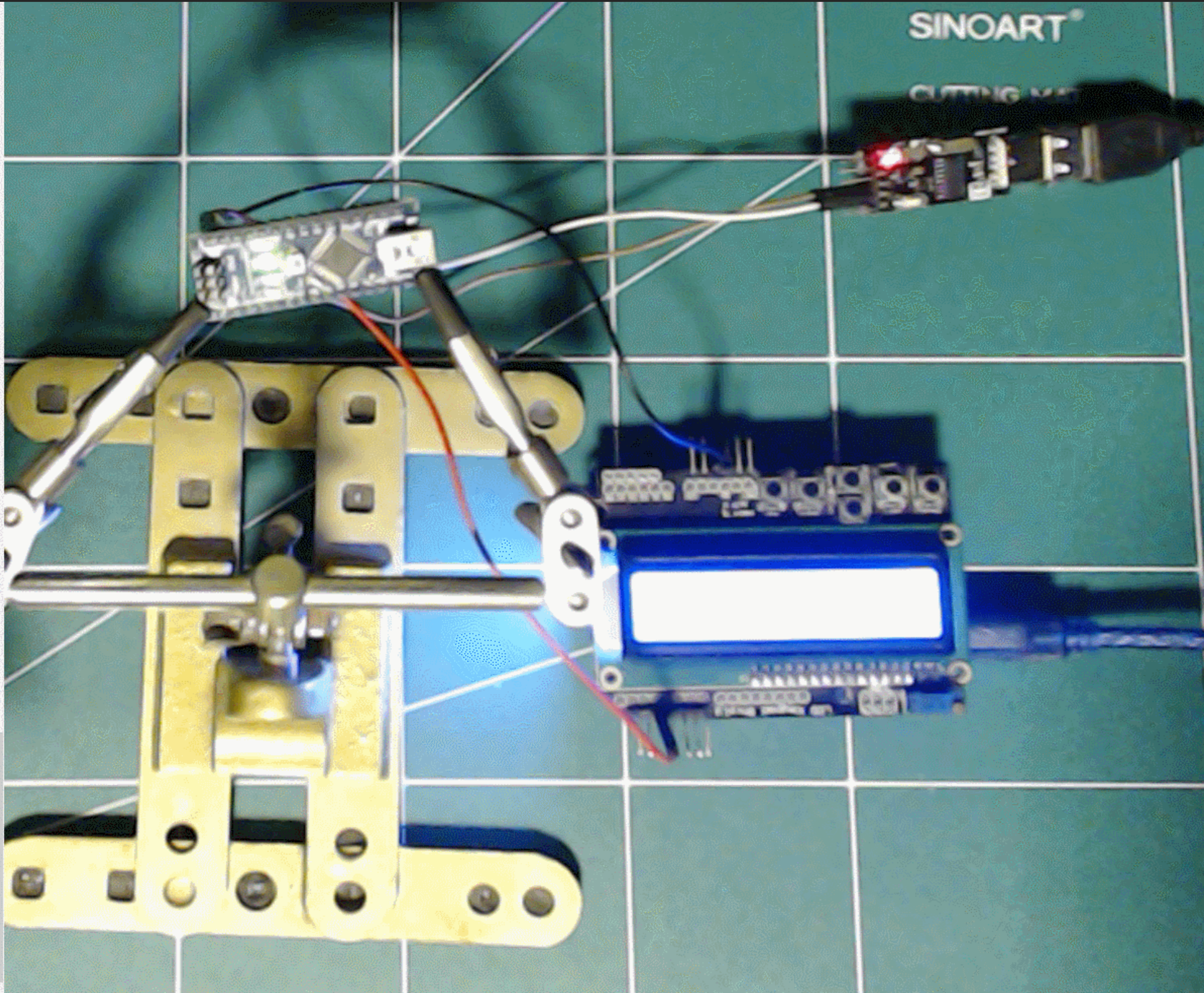
Como exemplo o circuito tenta ler um valor proveniente do barramento de dados antes que a memória tenha tempo de “definir” o valor requisitado. Outra possiblidade é que o circuito comece a executar a instrução n+1 antes que o microprocessador termine de executar a instrução n.



FONTE: https://www.slideshare.net/ZiyadAlshehri/fault-injection-attacks

Clock Fault Injection

```
kLockLockLockLockLockLockLockLockLock
LockLockLockLockLockLockLockLockLockL
ockLockLockLockLockLockLockLockLockLo
ckLockLockLockLockLockLockLockLockLoc
kLockLockLockLockLockLockLockLockLock
LockLockLockLockLockLockLockLockLockL
ockLockLockLockLockLockLockLockLockLo
ckLockLockLockLockLockLockLockLockLoc
kLockLockLockLockLockLockLockLockLock
LockLockLockLockLockLockLockLockLockL
ockLockLockLockLockLockLockLockLockLo
ckLockLockLockLockLockLockLockLockLoc
kLockLockLockLockLockLockLockLockLock
LockLockLockLockLockLockLockLockLockL
ockLockLockLockLockLockLockLockLockLo
ckLockLockLockLockLockLockLockLockLoc
kLockLockLockLockLockLockLockLockLock
LockLockLockLockLockLockLockLockLockL
ockLockLockLockLockLockLockLockLockLo
ckLockLockLockLockLockLockLockLockLoc
kLockLockLockLockLockLockLockLockLock
LockLockLockLockLockLockLockLockLockL
ockLockLockLockLockLockLockLockLockLo
ckLockLockLockLockLockLockLockLockLoc
kLockLockLockLockLockLockLockLockLock
LockLockLockLockLockLockLockLockLockL
ockLockLockLockLockLockLockLockLockLo
ckLockLockLockLockLockLockLockLockLoc
kLockLockLock
```

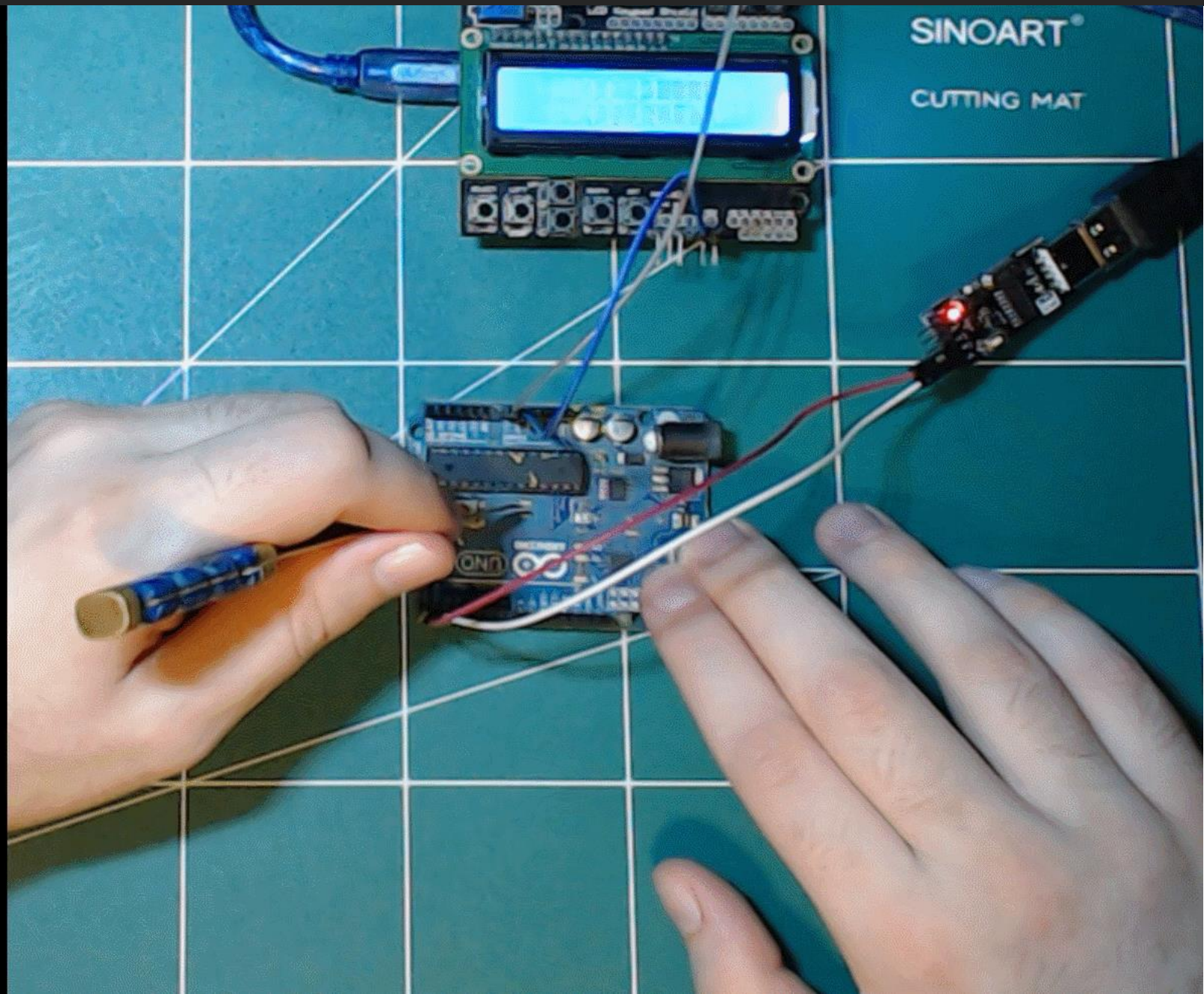


Entendendo o Código

```
1  int loopnumber = 0;
2  void setup() {
3    Serial.begin(9600);
4  }
5
6  void loop() {
7    int ctr = 0;
8    loopnumber++;
9    for(int i=0; i<500; i++){
10    for(int j=0; j<500; j++){
11      if (j % 100 == 0) {
12        ctr++;
13       }
14     }
15   }
16
17   Serial.print (loopnumber);
18   Serial.print (" - ");
19   Serial.print("controle: ");
20   Serial.println(ctr);
21 }
```

Clock Fault Injection (real)

```
1 - controle: 2500
2 - controle: 2500
3 - controle: 2500
4 - controle: 2500
1 - controle: 2500
2 - controle: 2500
3 - controle: 2500
1 - controle: 2500
2 - controle: 2500
2 - controle: 2500
3 - controle: 2500
4 - controle: 2500
5 - controle: 2500
6 - controle: 2500
7 - controle: 2500
8 - controle: 2500
9 - controle: 2500
10 - controle: 2500
11 - controle: 2500
12 - controle: 2500
13 - controle: 2500
14 - controle: 2500
15 - controle: 2500
16 - controle: 2500
17 - controle: 2500
18 - controle: 2500
19 - controle: 2500
20 - controle: 2500
21 - controle: 2500
```



Acerca do Ataque

Slides apresentados por Niek Timmers em 2016.

Fault injection fault model

riscure

Instruction corruption

```
MOV R0, R1          11100001101000000000000000000000
MOV R0, R2          11100001101000000000000000000010

MOV R0, R1          11100001101000000000000000000001
STR R7, [R7, #16]   11100101100010010111000000010000
```

Instruction skipping

```
MOV R0, R1          11100001101000000000000000000001
MOV R1, R1          11100001101000000010000000000001

MOV R0, R1          11100001101000000000000000000001
MOV R6, R6          11100001101000000110000000000110
```

Fault Models – ”Our” choice ...

When presented with code: ***instruction corruption****.*

Simple (MIPS)

```
addi $t1, $t1, 8    00100001001010010000000000001000
addi $t1, $t1, 0    00100001001010010000000000000000
```

Complex (ARM)

```
ldr w1, [sp, #0x8]  10111001010000000000101111100001
str w7, [sp, #0x20] 10111001000000000100101111100111
```

Remarks

- Limited control over which bit(s) will be corrupted
- May or may not be the true fault model
- Other fault model behavior covered

FONTE: https://pt.slideshare.net/riscure/controlling-pc-on-arm-using-fault-injection

Falha na Transmissão dos Dados

W25Q64BV

winbond

3. PIN CONFIGURATION SOIC 208-MIL

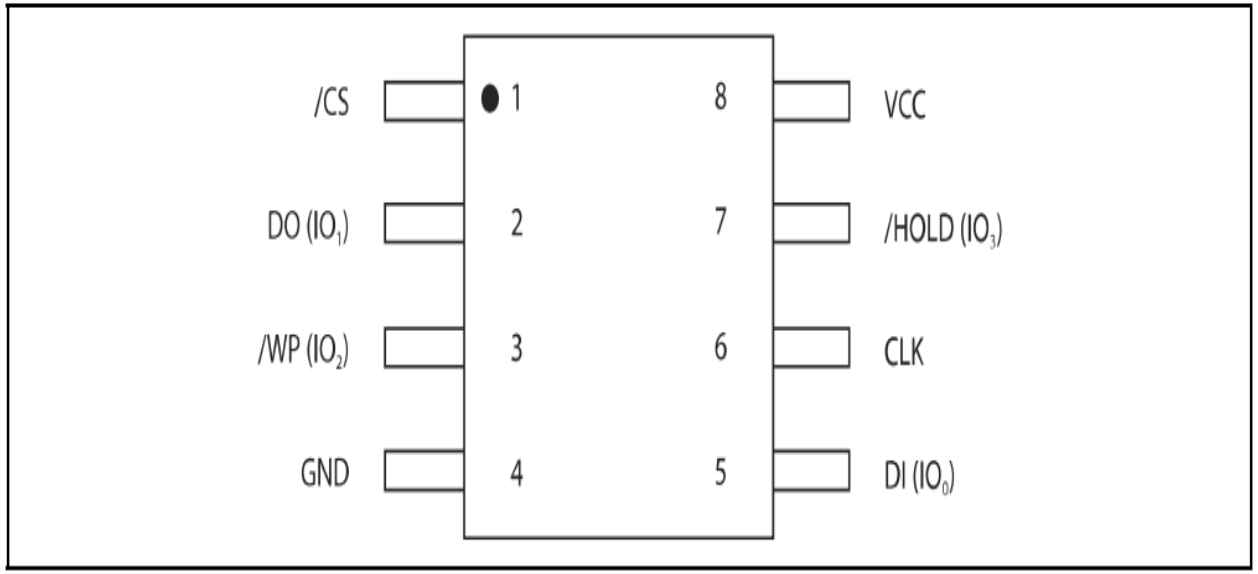
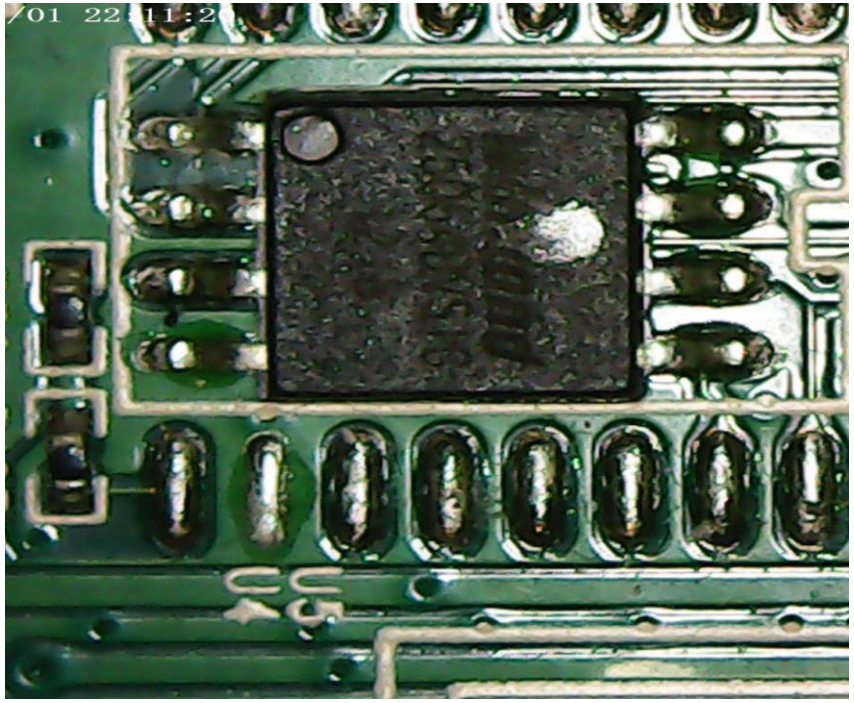
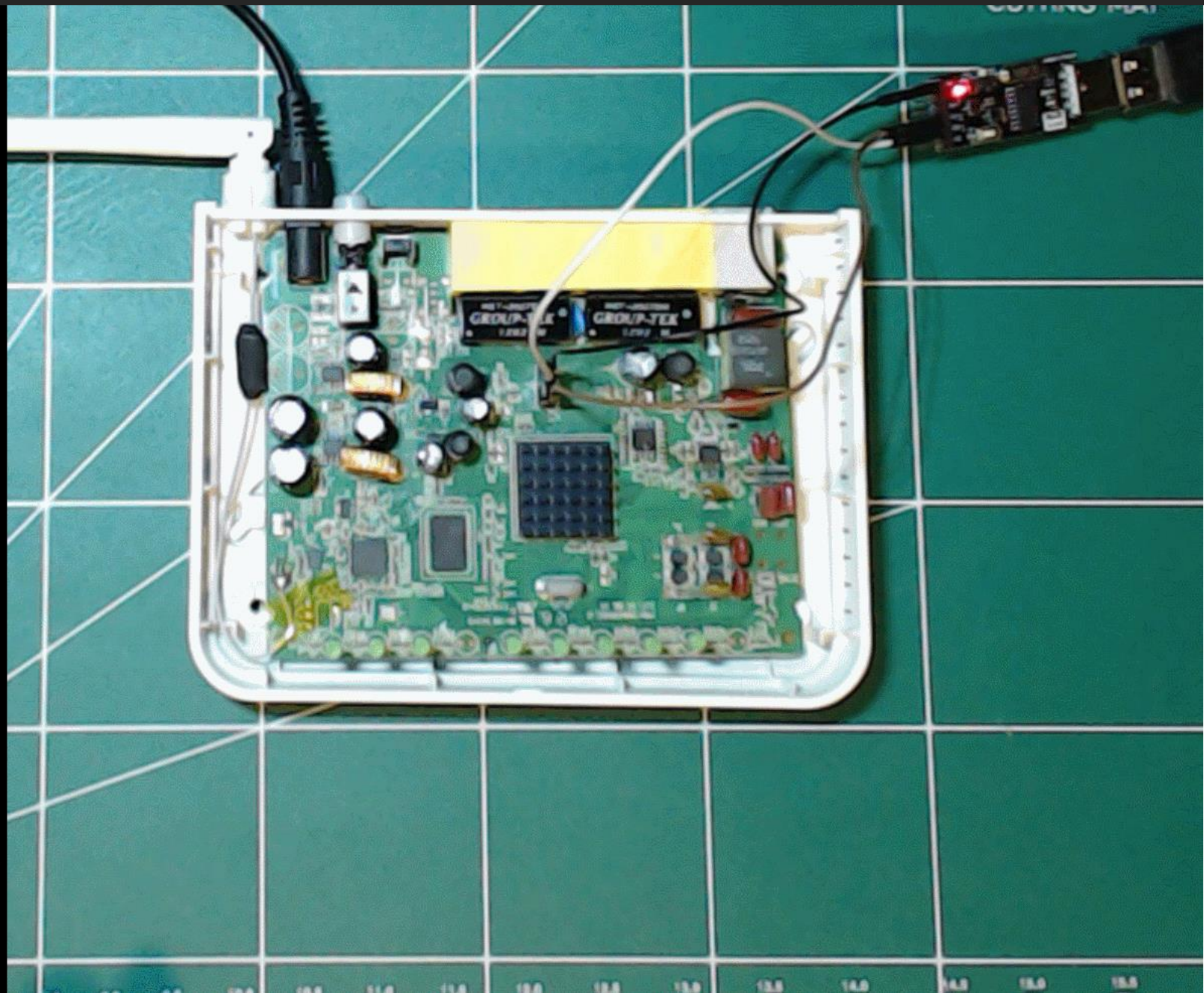


Figure 1a. W25Q64BV Pin Assignments, 8-pin SOIC 208-mil (Package Code SS)

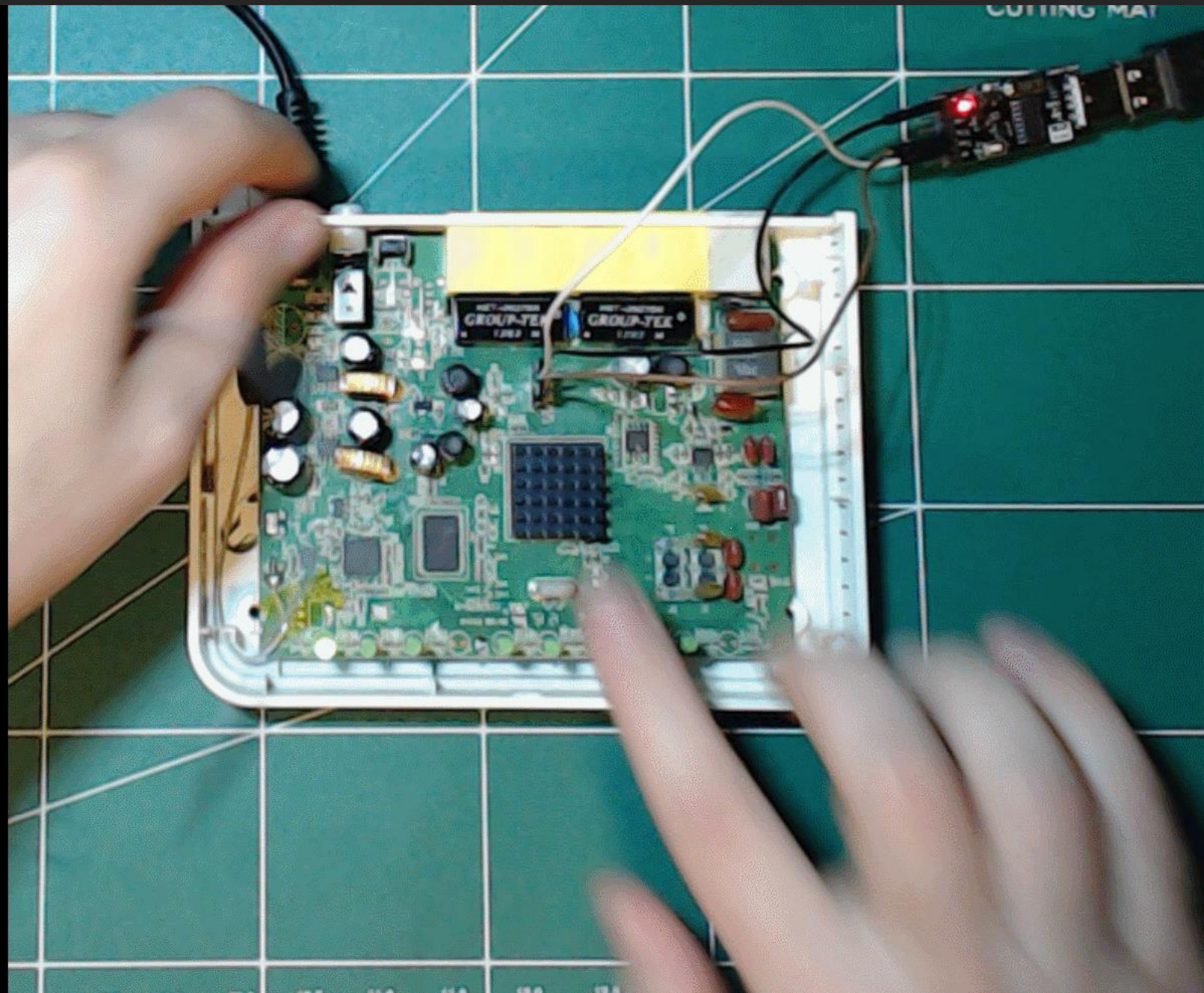


FONTE: https://www.youtube.com/watch?v=KRNTv3oXDkE

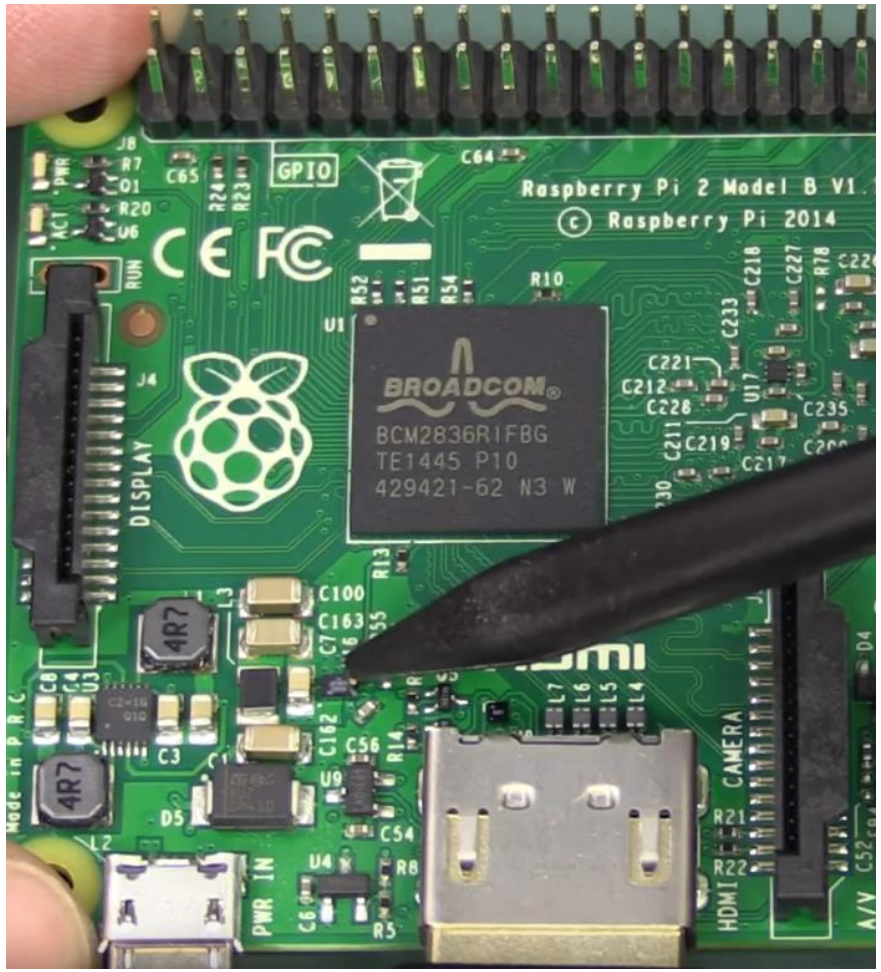
Funcionamento Normal



Causando Falhas no Carregamento do FS (pin2pwn)



Falha no Raspberry Pi 2



FONTE: https://www.youtube.com/watch?v=SrDfRCi1UV0

Heating Faults

No experimento em pauta, que é descrito por um ATmega162 com o sistema RSA implementado.

Foi possível através do aquecimento do micro controlador, extrair a chave privada utilizada no processo de criptografia.

Em temperaturas entre 152 e 158 ºC existe maior probabilidade de ocorrer um erro durante o cálculo do algoritmo.

Apenas uma falha durante o cálculo pode revelar os primos RSA (*p* e *q*).

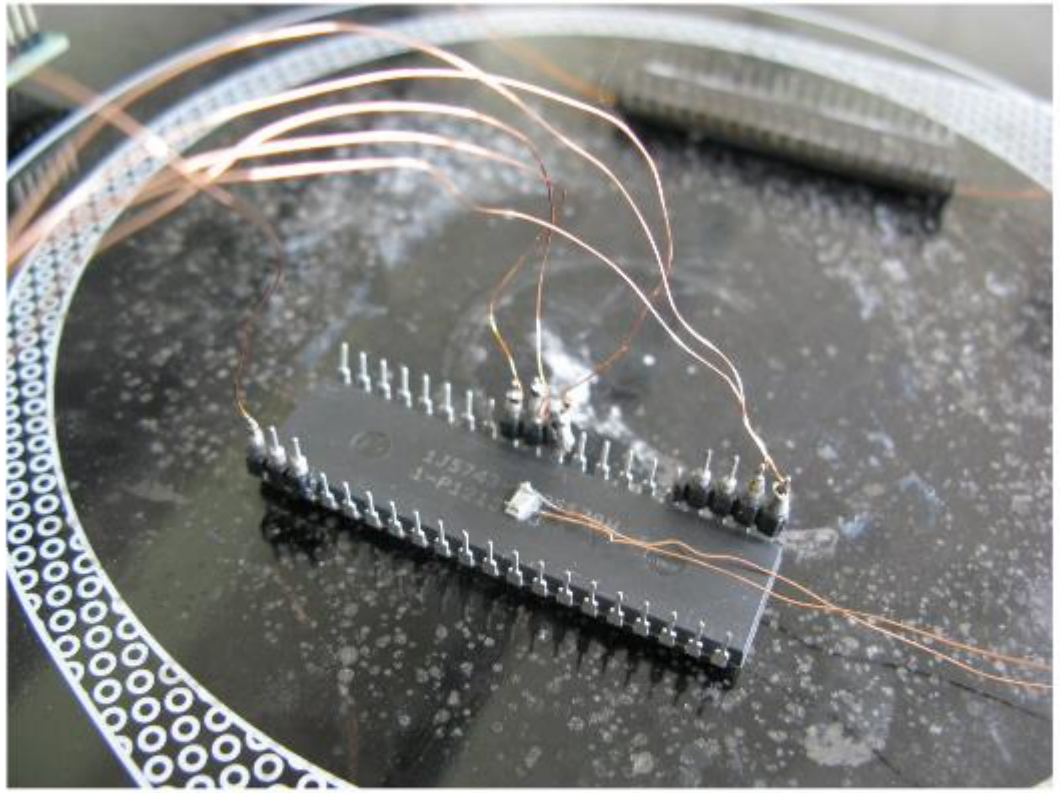
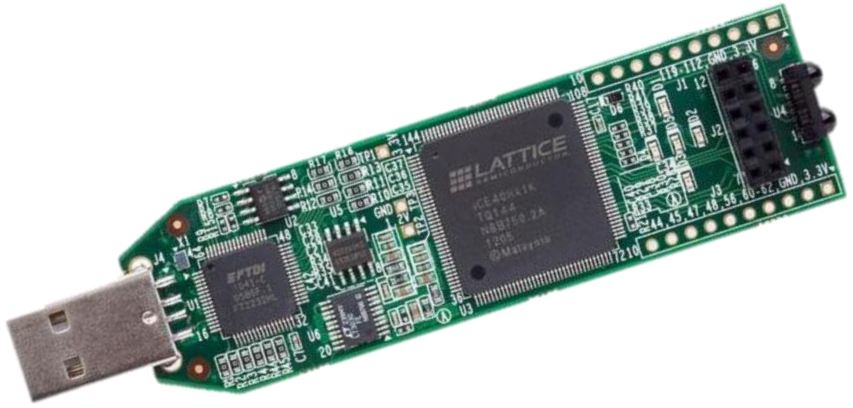
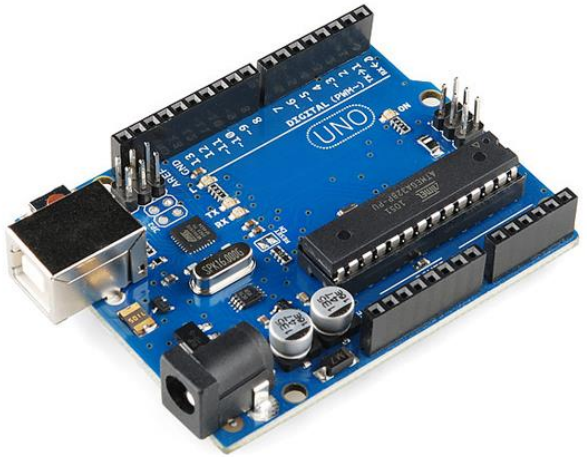


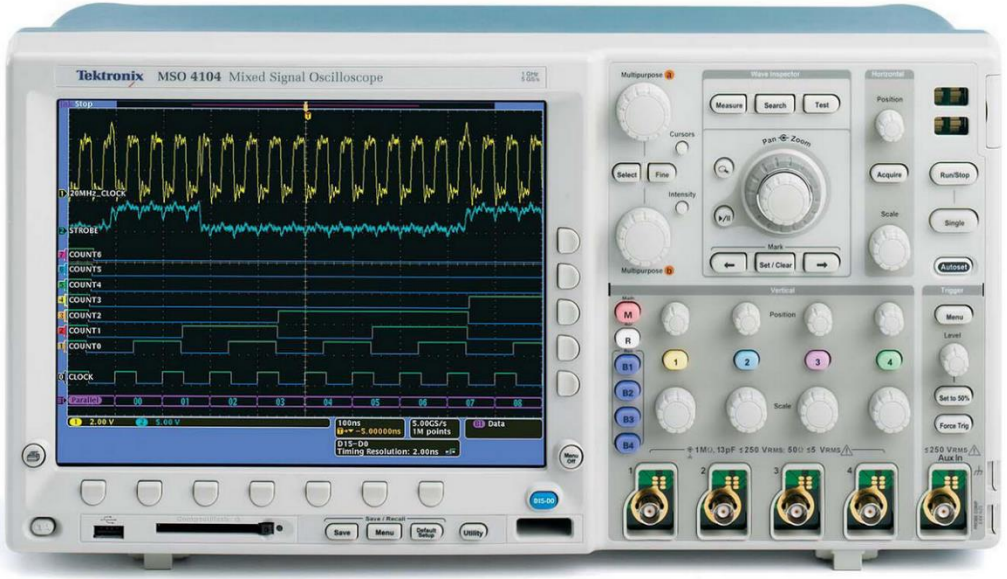
Fig. 6: Heating plate with two PT100 sensors measuring the rear-side and front-side temperature of an ATmega162.

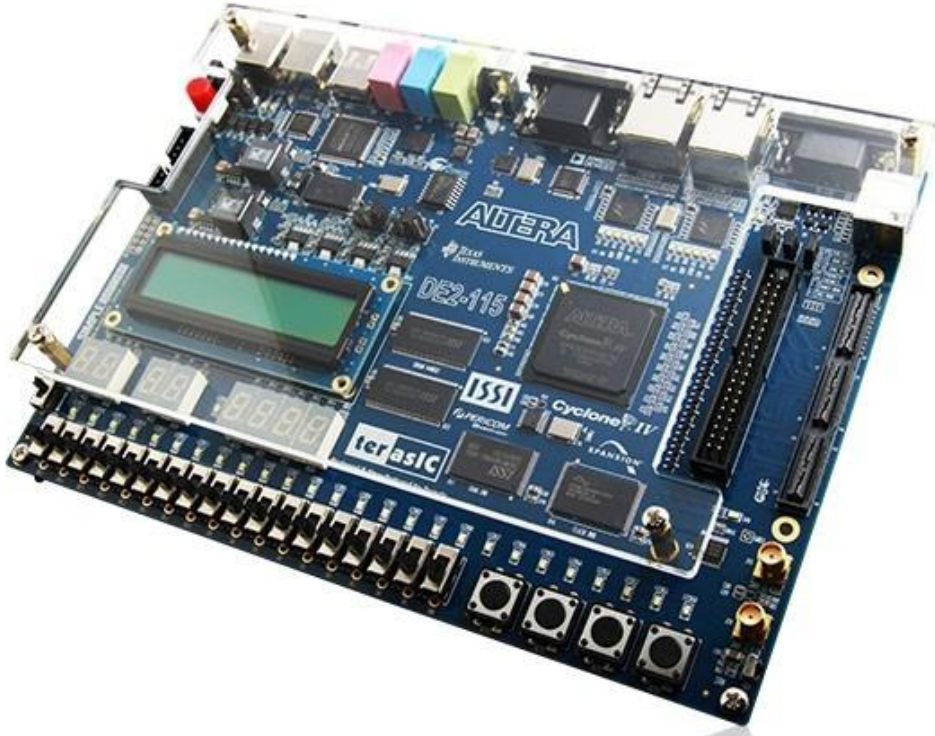
FONTE: https://eprint.iacr.org/2014/190.pdf

Equipamentos (até aqui blz)









Equipamentos

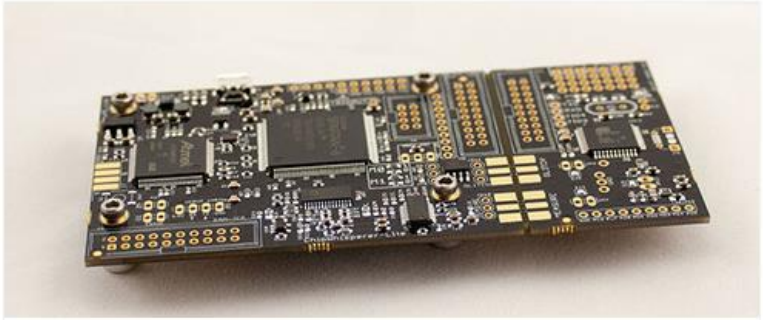
> 500k

Dear Julio,

Thank you very much for your email.

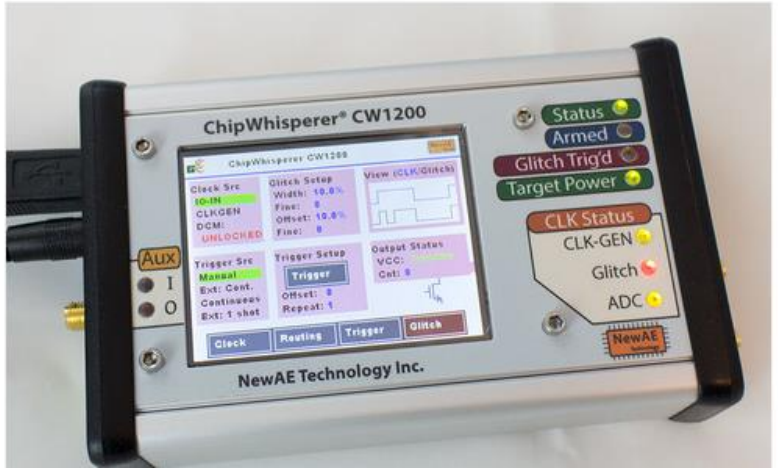
I have attached a generic slidedeck from our tools.

- Pricing for software is around 50k EUR per year (full SCA/FI suite with Deep Learning and server solutions).
- SCA hardware starts at 50k EUR including High End Scope and goes up to 250k EUR.
- FI hardware starts at 40k EUR for basic power glitching up to 500k EUR including double laser with 7 different laser sources.



ChipWhisperer-Lite (CW1173) Basic Board

$250.00



ChipWhisperer-Pro (Complete Level 3 Starter Kit)

$3,800.00

Product Description

ChipSHOUTER® Kit

$2,800.00

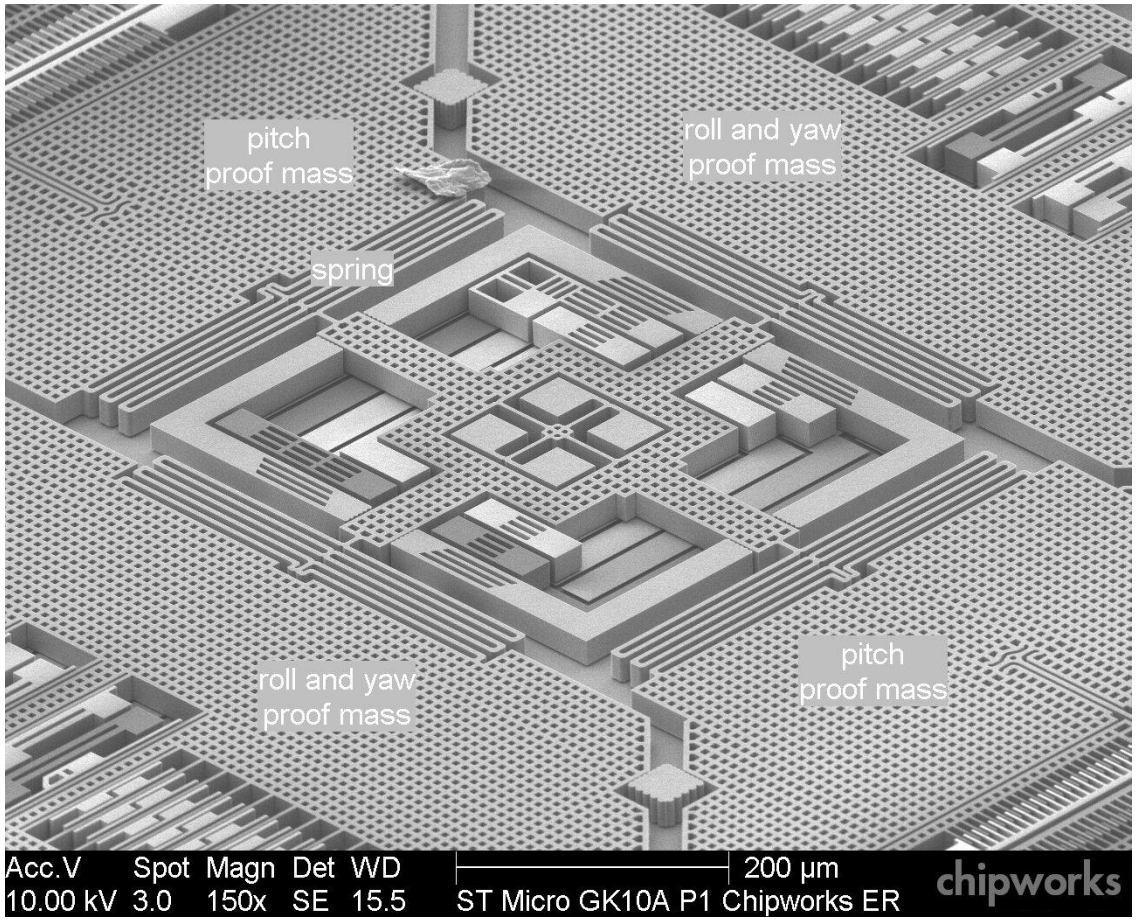
Product Description

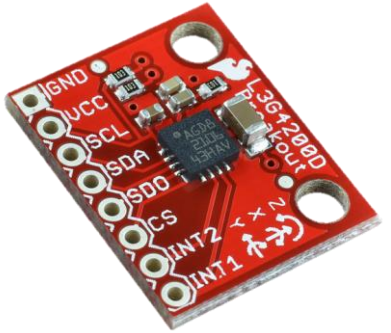
Falhas por Ultrassom

O objetivo é criar um efeito de ressonância em sistemas microeletromecânicos (MEMS, *microelectromechanical systems*), como giroscópios e acelerômetros.

Chips que utilizam a tecnologia MEMS são compostos por dispositivos mecânicos, eletrônicos, atuadores e sensores microscópicos que são encapsulados em chips.

A figura mostra a estrutura microscópica de um giroscópio MEMS L3G4200D.





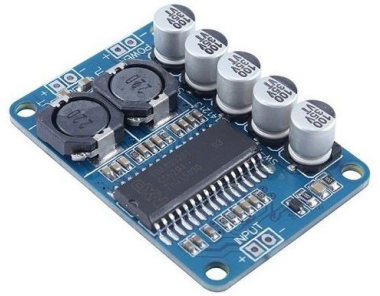
FONTE: https://www.youtube.com/watch?v=2g0gNzsoRYc

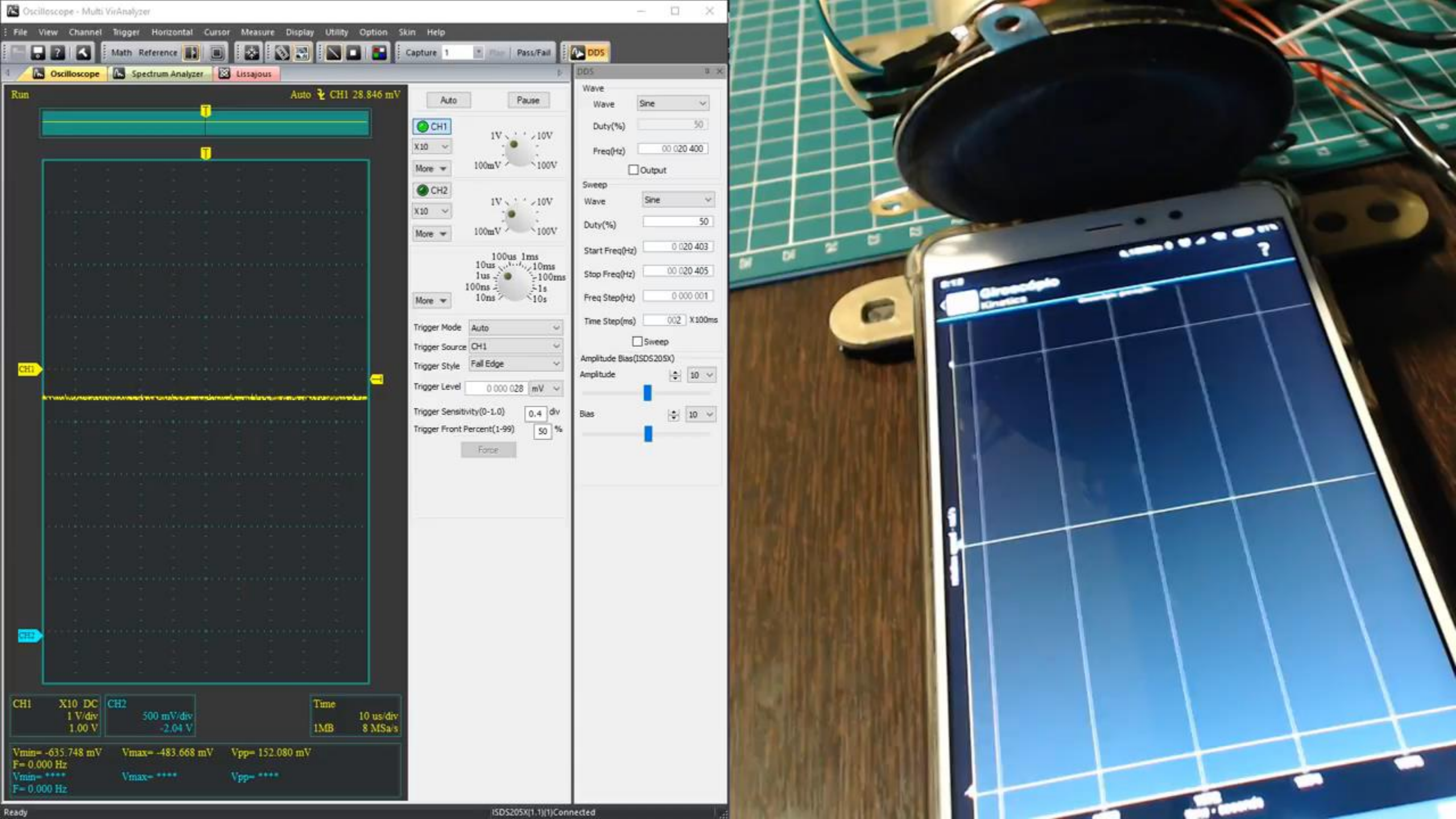
Objetivo do Ataque

Estimular a massa de detecção para que essa se mova mesmo com o eletrônico em repouso.

Para o experimento foram utilizados:

- Gerador de funções Instrustar modelo ISDS205X
- Módulo amplificador de áudio TDA8932
- Autofalante ou transdutor ultrassônico
- Smartphone Xiaomi Mi5s Plus (alvo)



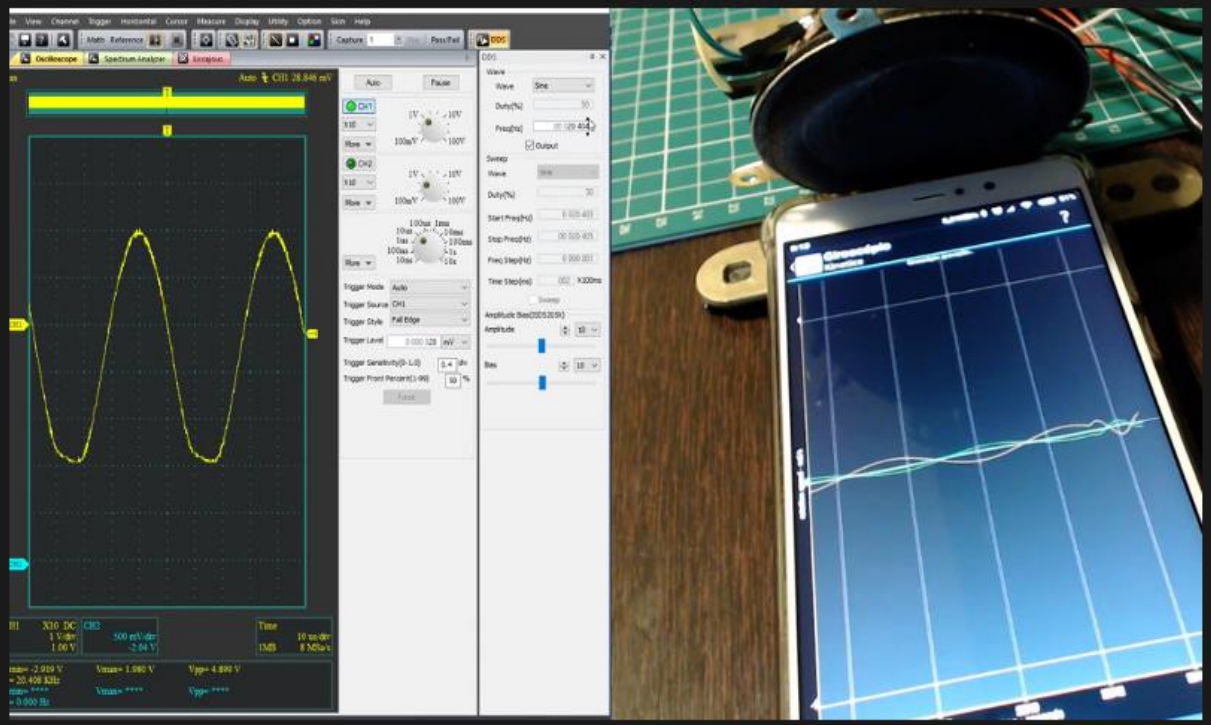

Oscilloscope - Multi VirAnalyzer
File View Channel Trigger Horizontal Cursor Measure Display Utility Option Skin Help
Math Reference
Capture 1
Pass/Fail
DDS
Oscilloscope
Spectrum Analyzer
Lissajous
Run
Auto CH1 28.846 mV
CH1
CH2
Auto
Pause
X10
More
1V 10V 100mV 100V
100us 1ms 10us 10ms 1us 100ms 100ns 1s 10ns 10s
Trigger Mode Auto
Trigger Source CH1
Trigger Style Fall Edge
Trigger Level 0.000 028 mV
Trigger Sensitivity(0-1.0) 0.4 div
Trigger Front Percent(1-99) 50 %
Force
DDS
Wave
Wave Sine
Duty(%) 50
Freq(Hz) 00 020 400
Output
Sweep
Wave Sine
Duty(%) 50
Start Freq(Hz) 0 020 403
Stop Freq(Hz) 00 020 405
Freq Step(Hz) 0.000 001
Time Step(ms) 002 X100ms
Sweep
Amplitude Bias(ISDS205X)
Amplitude 10
Bias 10
CH1 X10 DC 1 V/div 1.00 V
CH2 500 mV/div -2.04 V
Time 10 us/div 1MB 8 MSa/s
Vmin= -635.748 mV Vmax= -483.668 mV Vpp= 152.080 mV
F= 0.000 Hz
Vmin= **** Vmax= **** Vpp= ****
F= 0.000 Hz
Ready
ISDS205X(1.1)(1)Connected

FREAK OUT YOUR SMARTPHONE WITH ULTRASOUND

by: Tom Nardi

13 Comments

July 17, 2018



LOGIC ANALYZERS FOR FPGAS: A VERILOG ODYSSEY

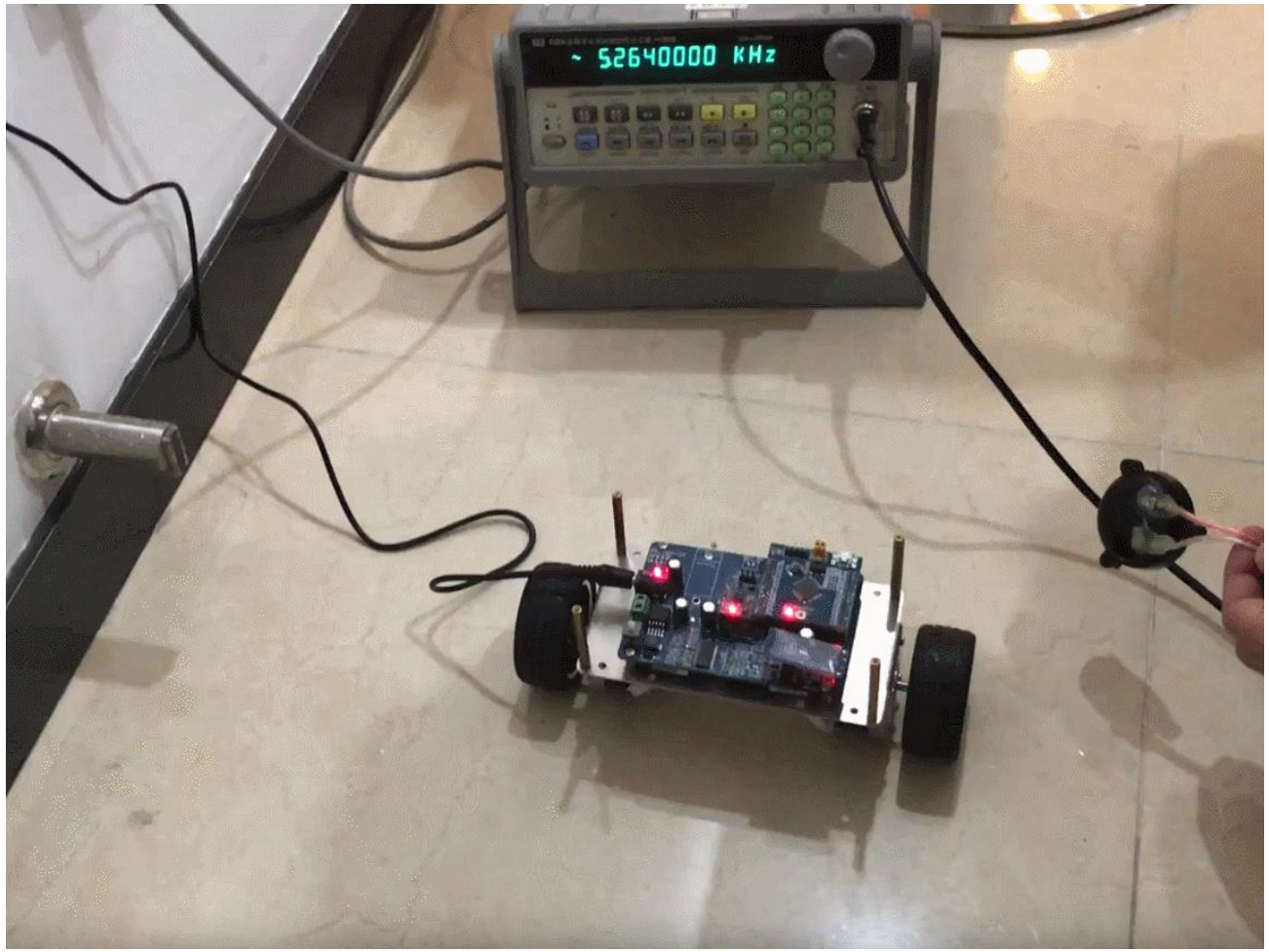
10 Comments

INTERNATIONAL SPACE STATION IS RACING THE CLOCK AFTER SOYUZ

Algumas Conclusões

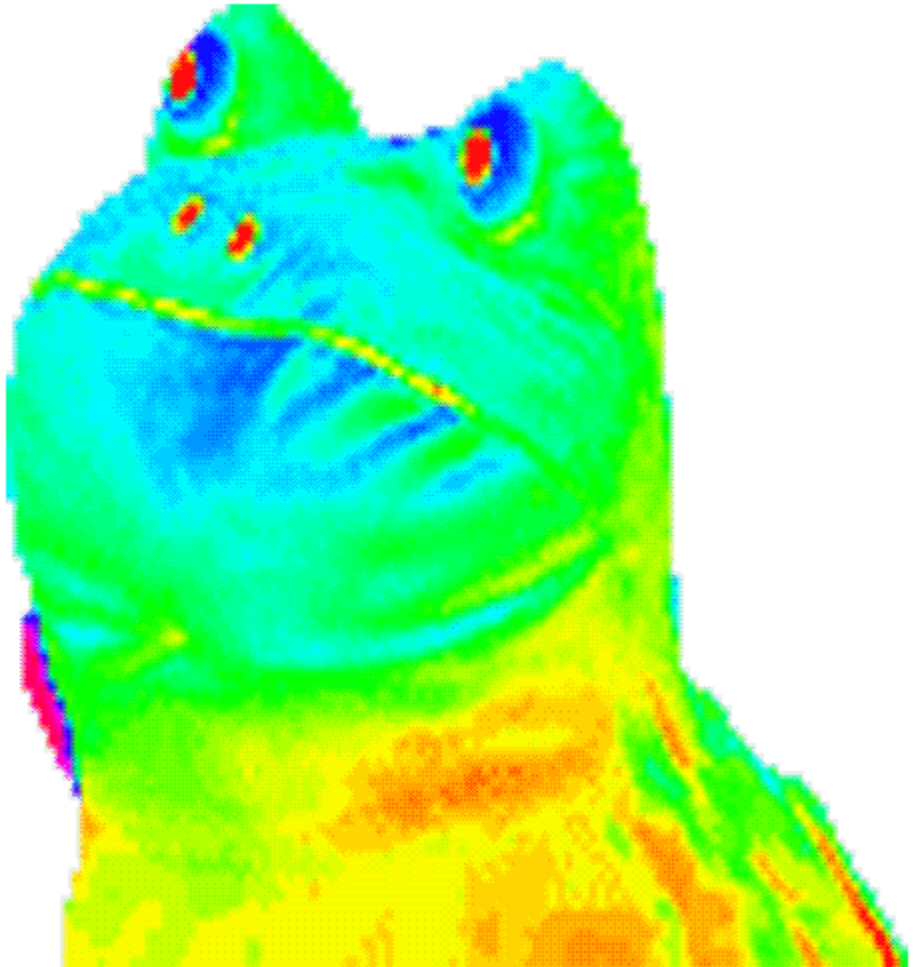
Foi possível arbitrar um padrão de ressonância no celular alvo com certa facilidade, o smartphone testado é um modelo relativamente recente.

Muitos outros dispositivos utilizam MEMS similares e podem ser explorados da mesma forma.



FONTE: https://www.blackhat.com/docs/us-17/thursday/us-17-Wang-Sonic-Gun-To-Smart-Devices-Your-Devices-Lose-Control-Under-Ultrasound-Or-Sound.pdf

Obrigado!!!



https://www.facebook.com/juliodellaflora

https://www.linkedin.com/in/juliodellaflora

https://twitter.com/jcldf