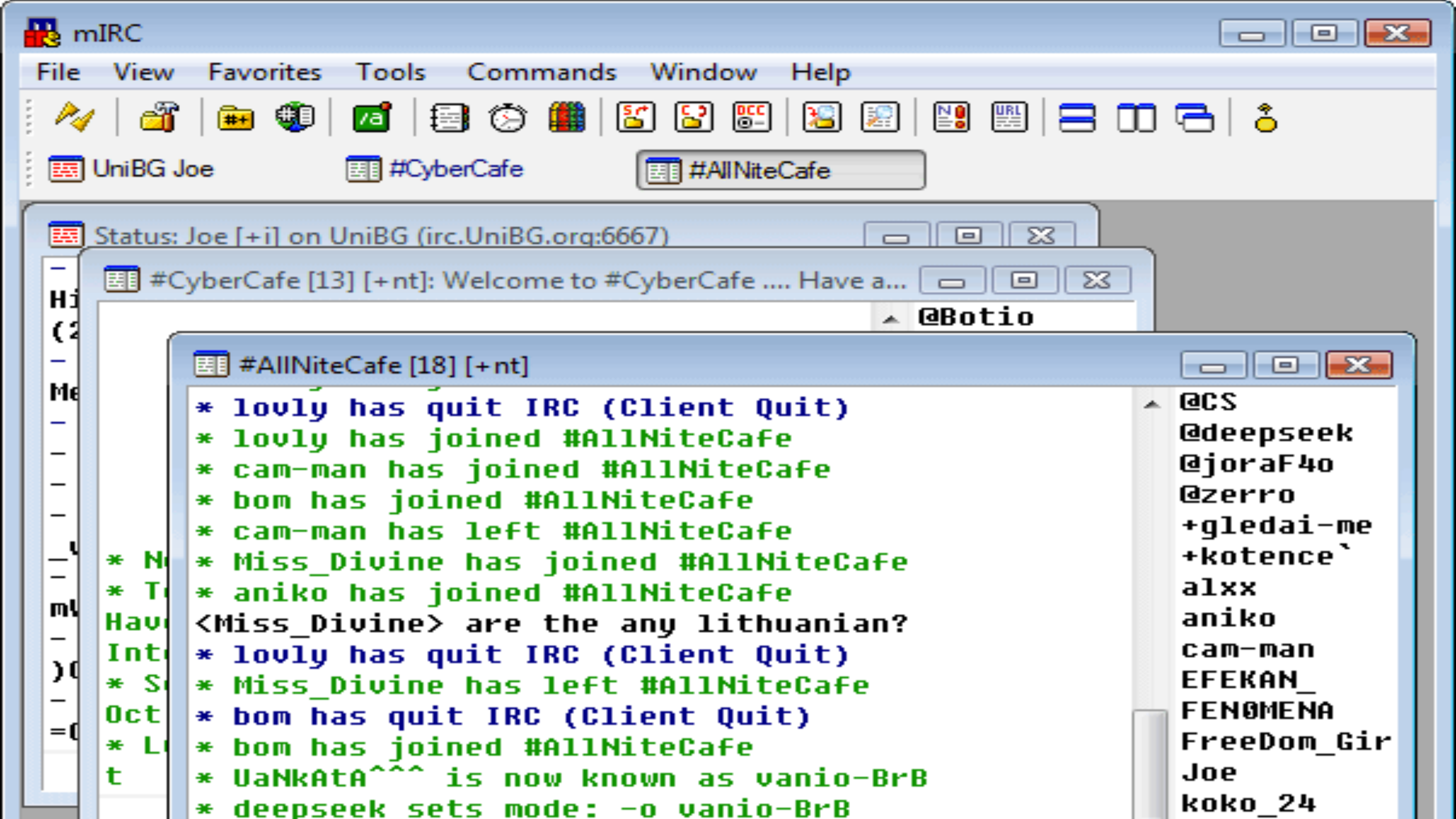
latest @ samy.pl/dc32

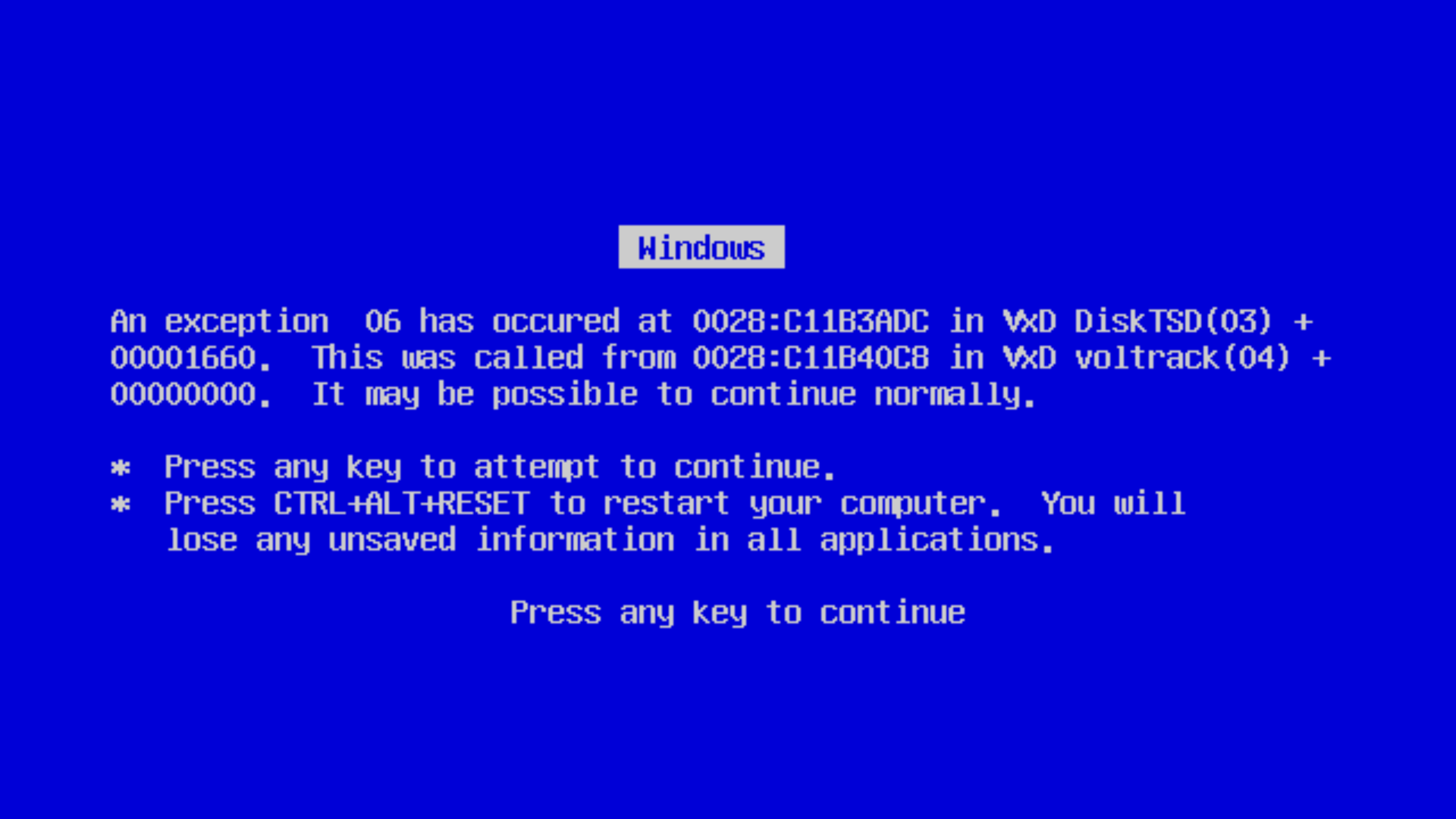
Optical Espionage

(and other ways to exploit physics)

@samykamkar
samy.pl


C90
Videon
speed


mIRC
File View Favorites Tools Commands Window Help
UniBG Joe
#CyberCafe
#AllNiteCafe
Status: Joe [+i] on UniBG (irc.UniBG.org:6667)
#CyberCafe [13] [+nt]: Welcome to #CyberCafe .... Have a...
@Botio
#AllNiteCafe [18] [+nt]
* lovly has quit IRC (Client Quit)
* lovly has joined #AllNiteCafe
* cam-man has joined #AllNiteCafe
* bom has joined #AllNiteCafe
* cam-man has left #AllNiteCafe
* Miss_Divine has joined #AllNiteCafe
* aniko has joined #AllNiteCafe
<Miss_Divine> are the any lithuanian?
* lovly has quit IRC (Client Quit)
* Miss_Divine has left #AllNiteCafe
* bom has quit IRC (Client Quit)
* bom has joined #AllNiteCafe
* UaNkAtA^^^ is now known as vanio-BrB
* deepseek sets mode: -o vanio-BrB
@CS
@deepseek
@joraF4o
@zerro
+gledai-me
+kotence`
alxx
aniko
cam-man
EFEKAN_
FEN0MENA
FreeDom_Gir
Joe
koko_24


Windows
An exception 06 has occured at 0028:C11B3ADC in VxD DiskTSD(03) +
00001660. This was called from 0028:C11B40C8 in VxD voltrack(04) +
00000000. It may be possible to continue normally.
* Press any key to attempt to continue.
* Press CTRL+ALT+RESET to restart your computer. You will
lose any unsaved information in all applications.
Press any key to continue

An exception
00001660. T
00000000. I

* Press any
* Press CTR
lose any

skTSD(03) +
ltrack(04) +

will

WinnukeV95



WinNuke V95
(c)1997 BurntBogus of the Den
Greets to Hound Dog

Nuke ME 95

NUKE IP ADDRESS
10.0.0.1

NUKE WITH MESSAGE
Greetings !

Exit

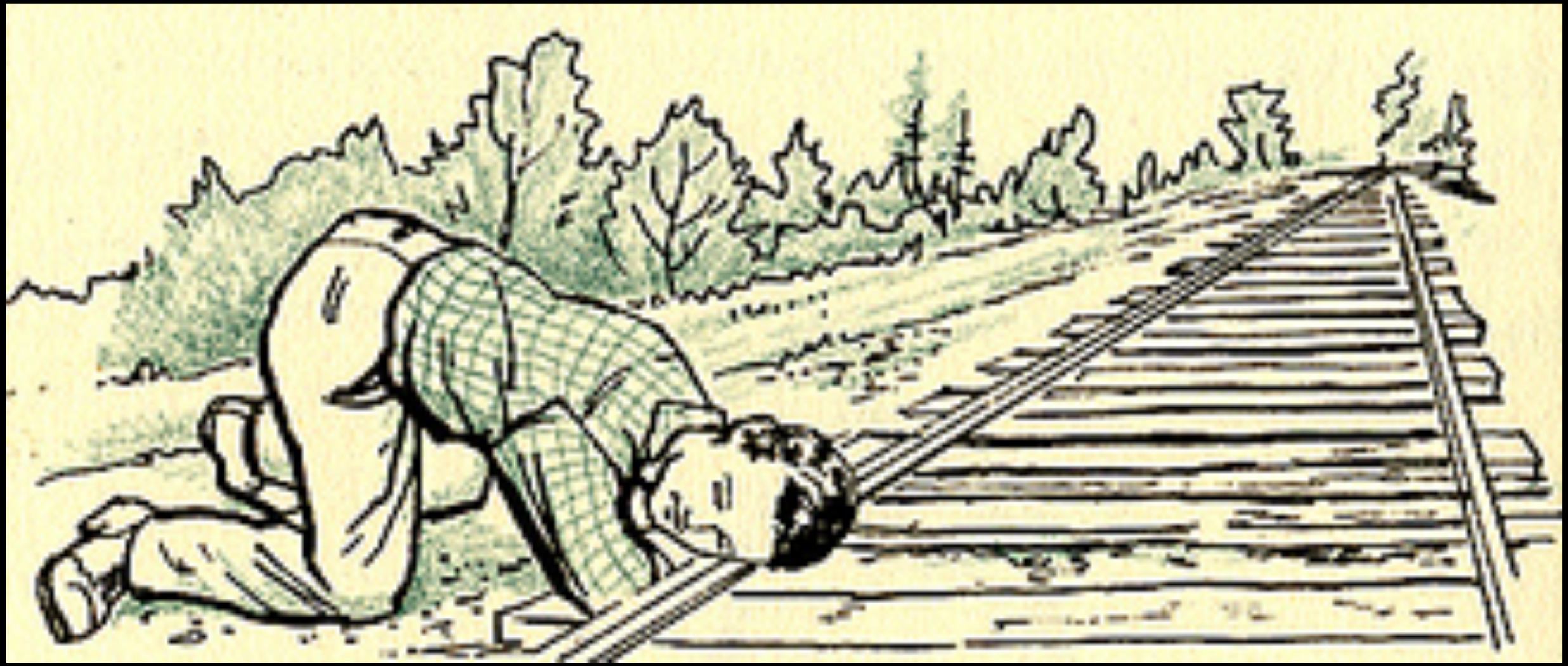


.:: Introduction ::.

Issues: [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23]
[24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45]
[46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [67]
[68] [69] [70]

Current issue : #49 | Release date : 1996-11-08 | Editor : daemon9 Get tar.gz

ground truth





example from @jzvw


TILT


MISSED
MISSED
HOW TO OPERATE
SCORE VOIDED IF MACHINE HAS BEEN TILTED
2 - Push RED knob to elevate ball to playing surface.
3 - Pull back BLACK knob on plunger and release.
example from @jzvw

energy

energy

==

information

light

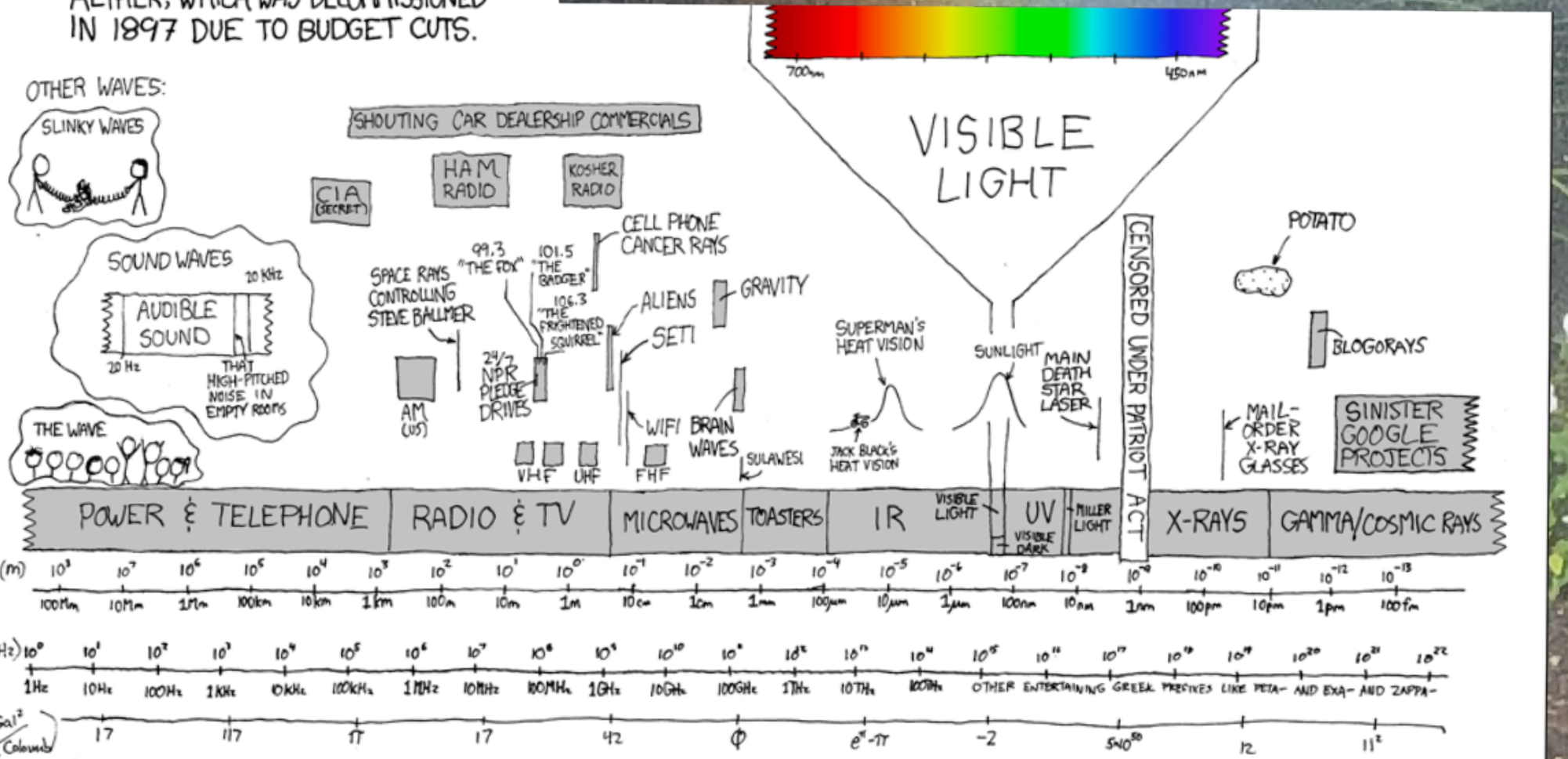




THE ELECTROMAGNETIC SPECTRUM

THESE WAVES TRAVEL THROUGH THE ELECTROMAGNETIC FIELD. THEY WERE FORMERLY CARRIED BY THE AETHER, WHICH WAS DECOMMISSIONED IN 1897 DUE TO BUDGET CUTS.





xkcd.com/273/

light

—

infrared

infra- from Latin, “below”



“In my experience, once data becomes invisible, something magical happens: they forget about security”

- Adam "Major Malfunction" Laurie

adamsblog.aperturelabs.com/2013_03_01_archive.html

light

visible

STEM
@stem_feed

Isaac Newton designing the cover for Pink Floyd's album.



twitter.com/stem_feed/status/1533465304654700544

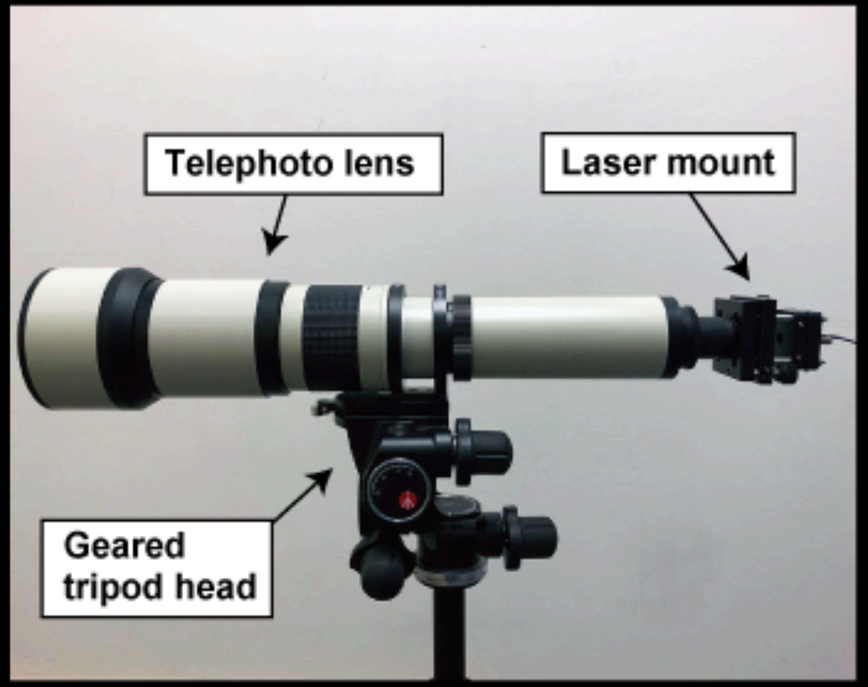
The Dark Side of the Moon

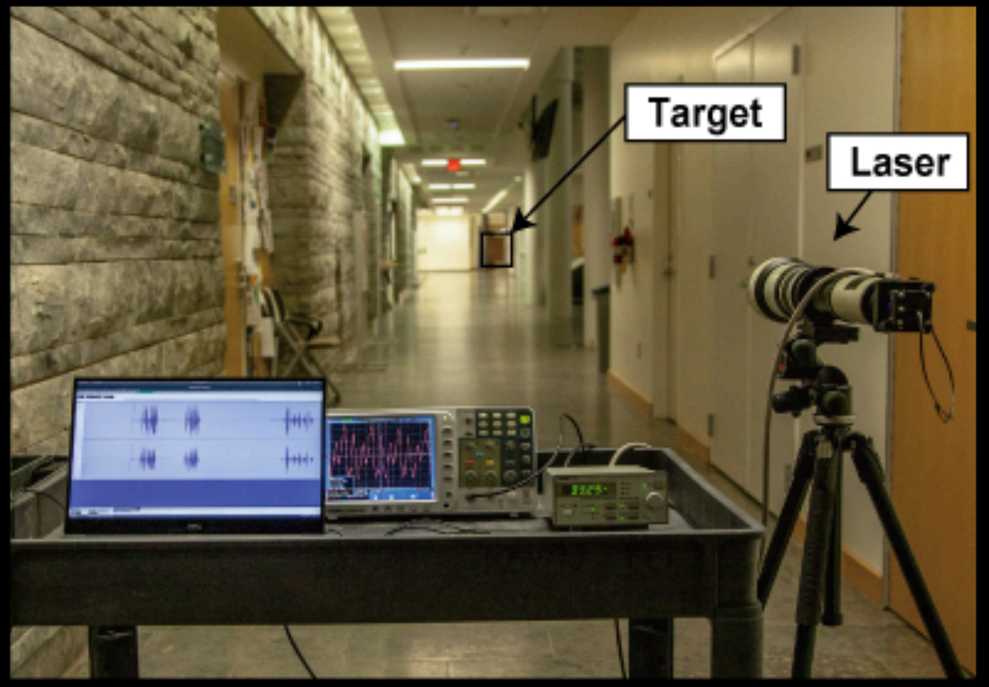


Studio album by Pink Floyd

Released	1 March 1973
Recorded	31 May 1972 – 9 February 1973[1]

visible light fault injection







lightcommands.com/20191104-Light-Commands.pdf

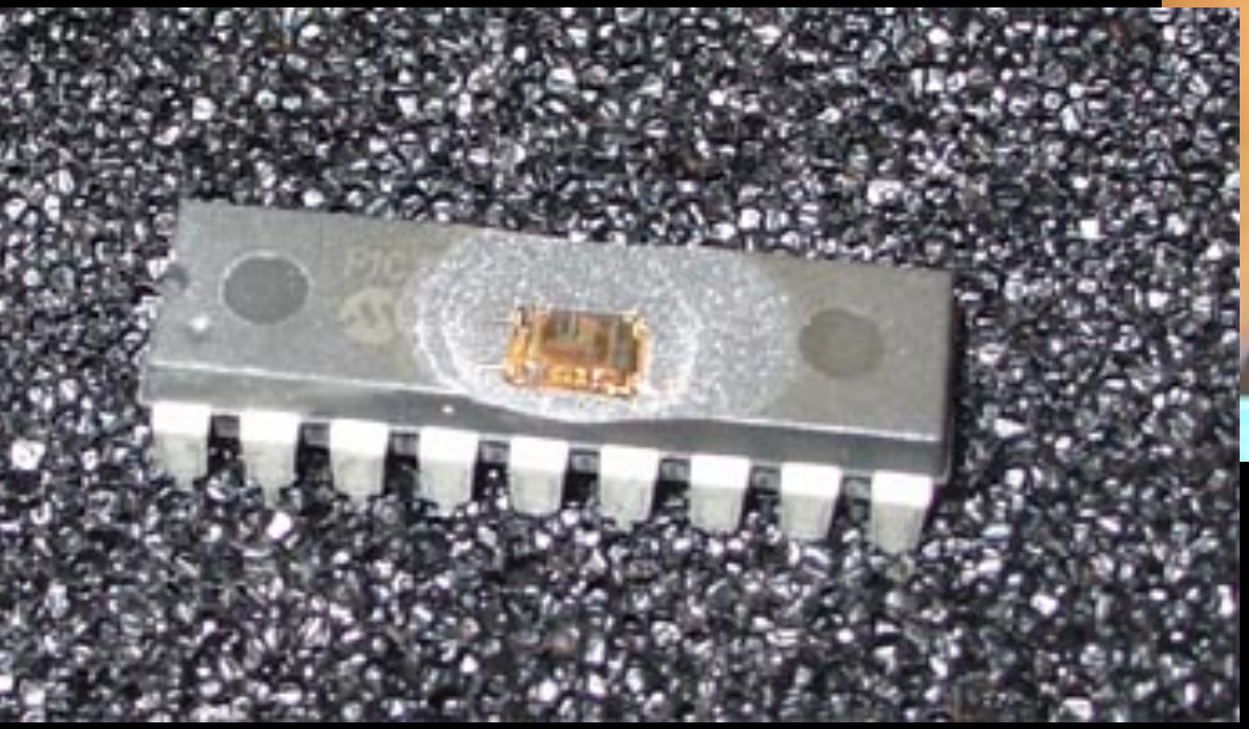
light

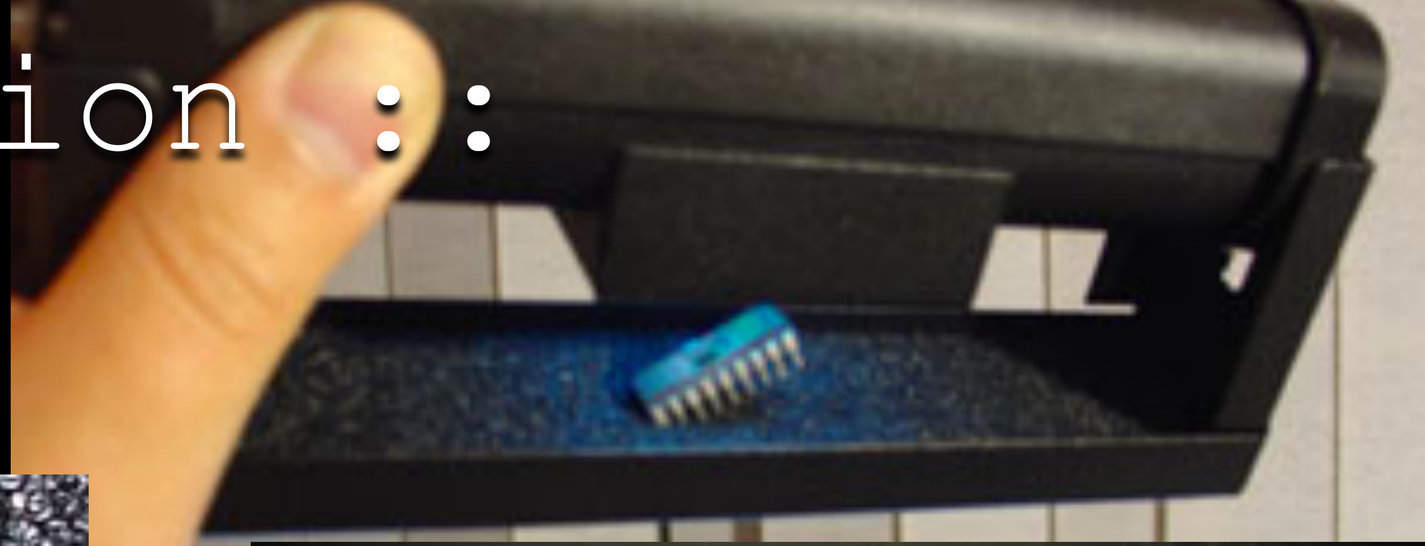
---

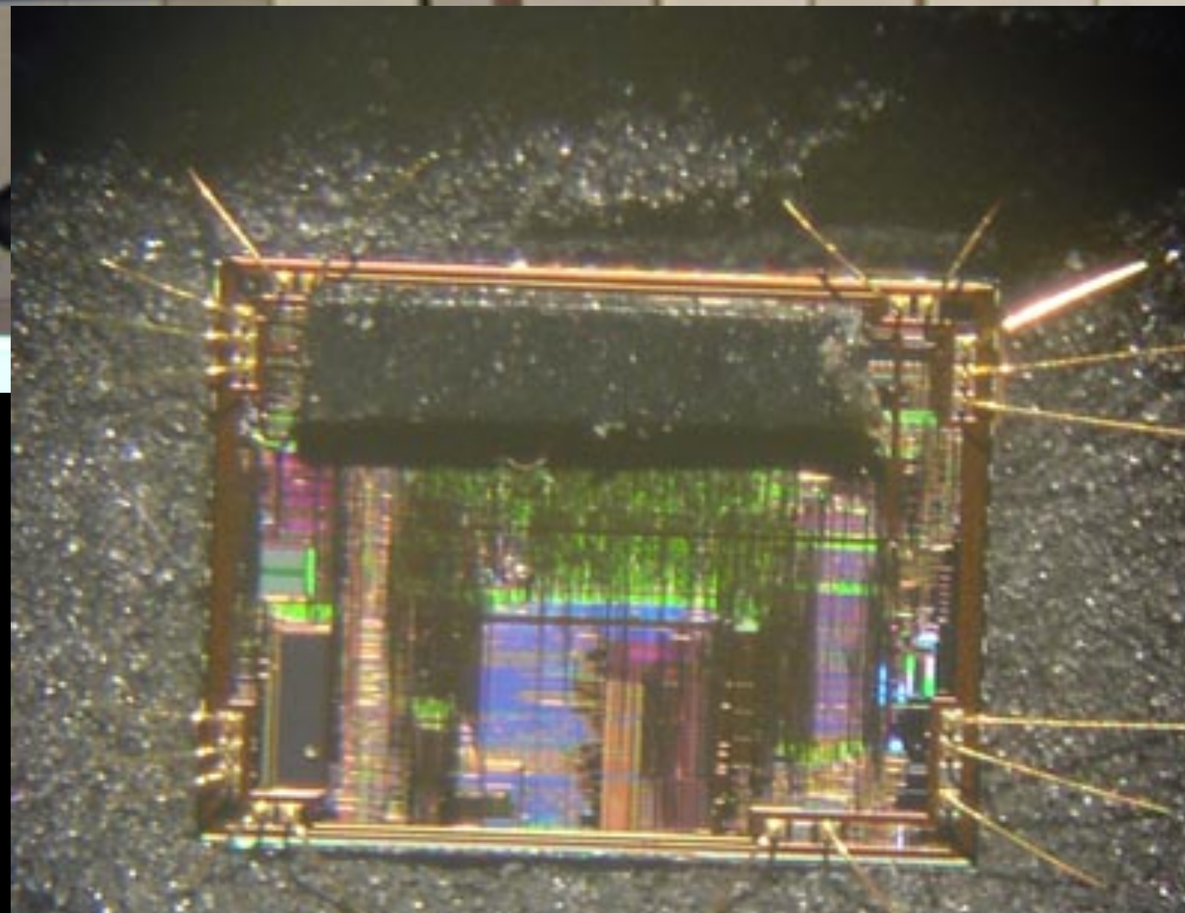
ultraviolet

ultra- from Latin
“beyond” or “on the far side of"

fault injection :: ultraviolet

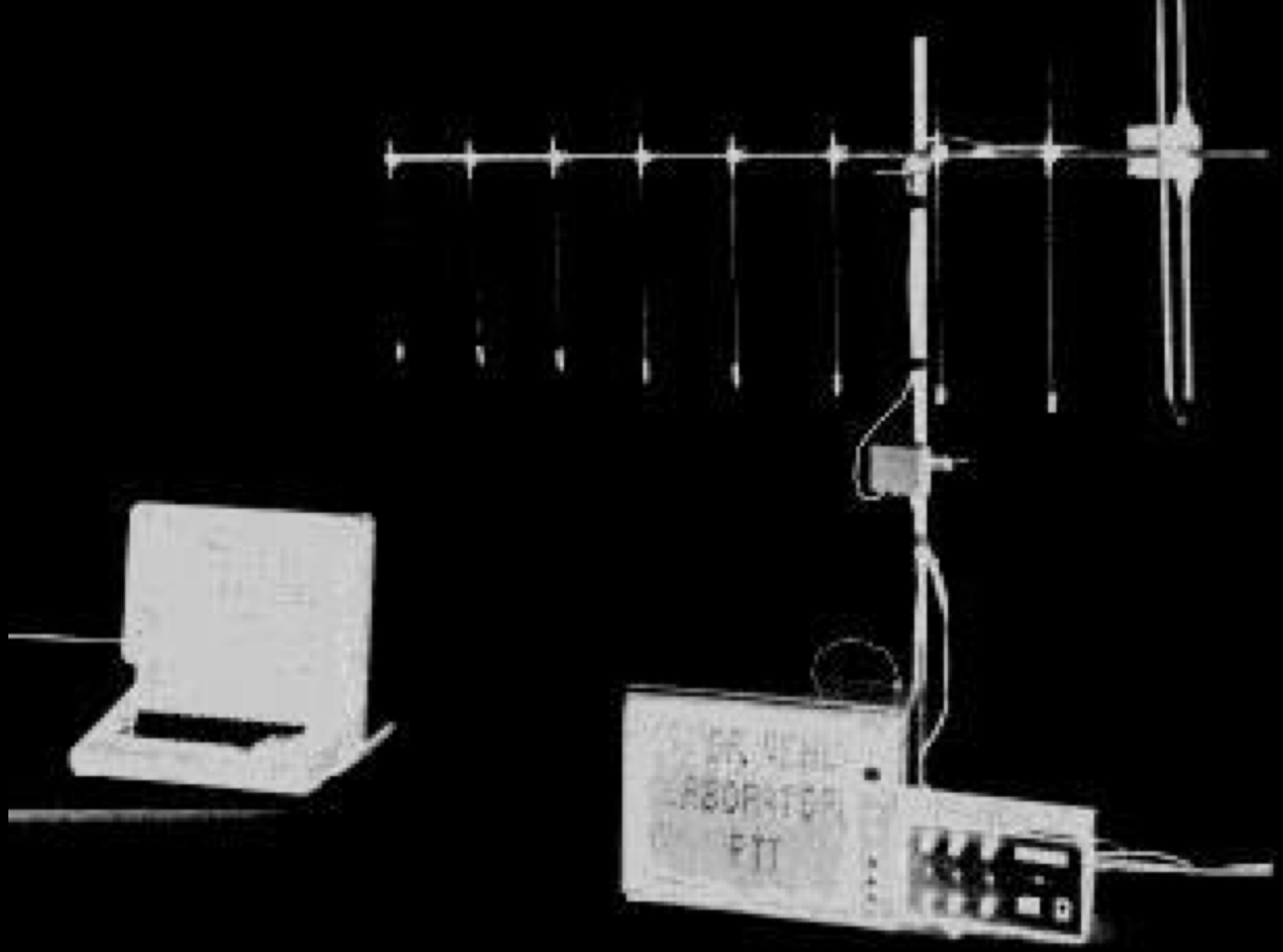






www.bunniestudios.com/blog/?page_id=40

radio



nsa.gov/ REDACTED frequency/ REDACTED pdf

electro-magnetism

electro-magnetism

electro- from Greek ‘ēlektron’, “amber”

electro-magnetism

electro- from Greek ‘ēlektron’, “amber”
magnetism from ‘magnētis lithos’, "Magnesian stone"

electro-magnetism

light + radio



https://samy.pl/magspoof

Use of this card is subject to the cardmember agreement. 140259H 04/14 4147-12-170-52

chase.com/freedom | 1-800-524-3880 | Int'l Collect: 1-302-594-8200 | Español: 1-888-446-3308



Not

CHASE

https://samy.pl/magspoof



https://samy.pl/magspoof

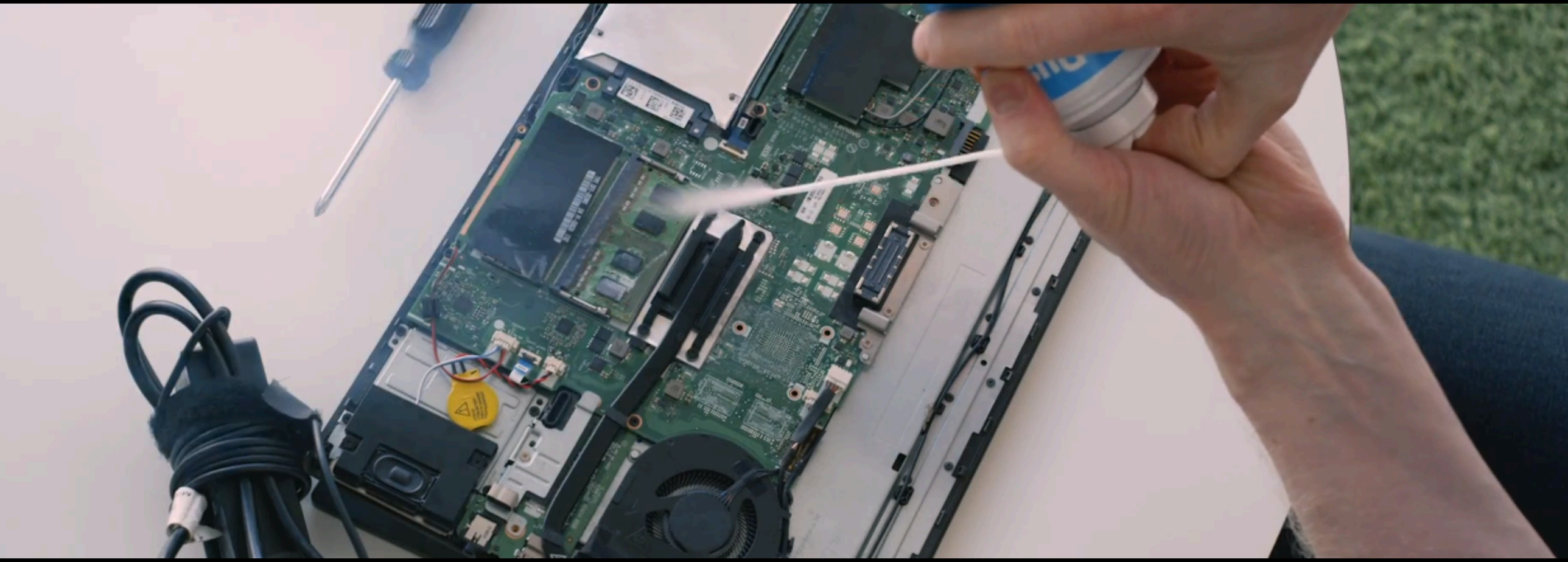
temperature

side channel ::
infrared (IR)



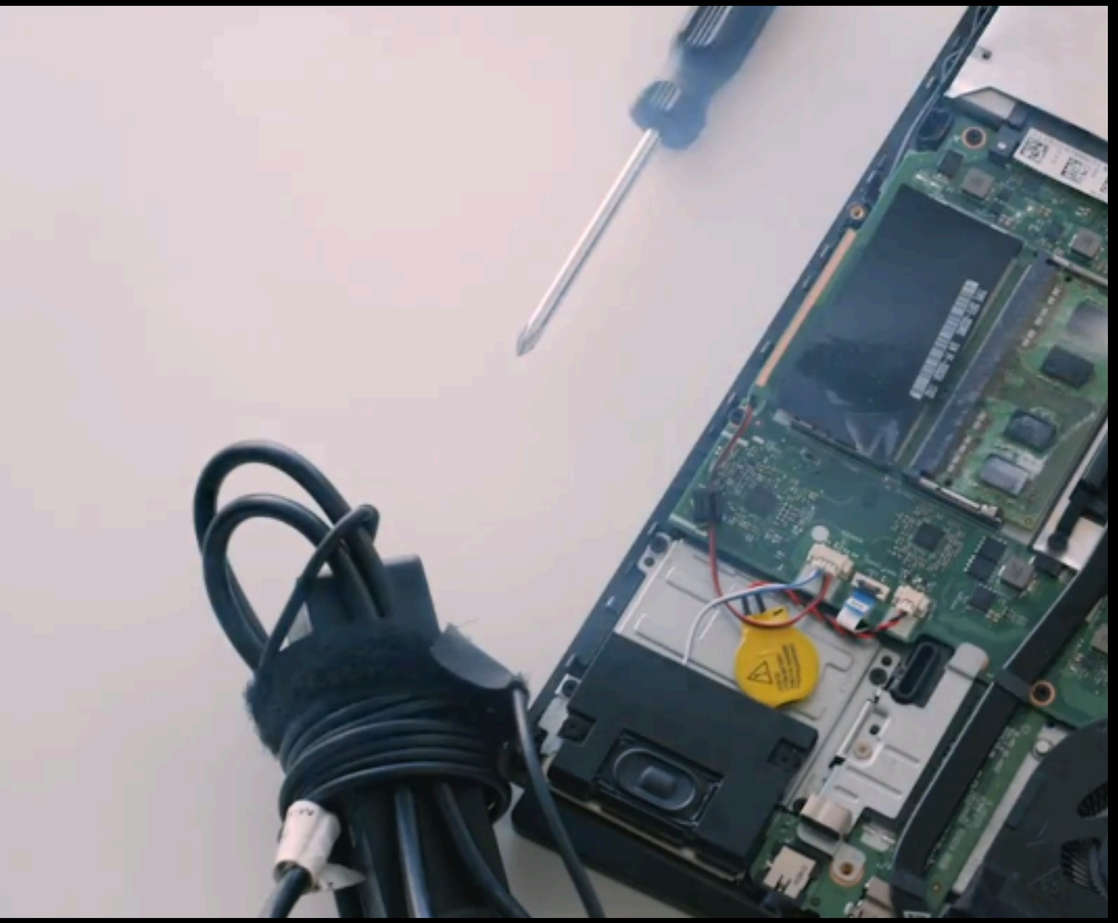
youtu.be/8Vc-69M-UWk

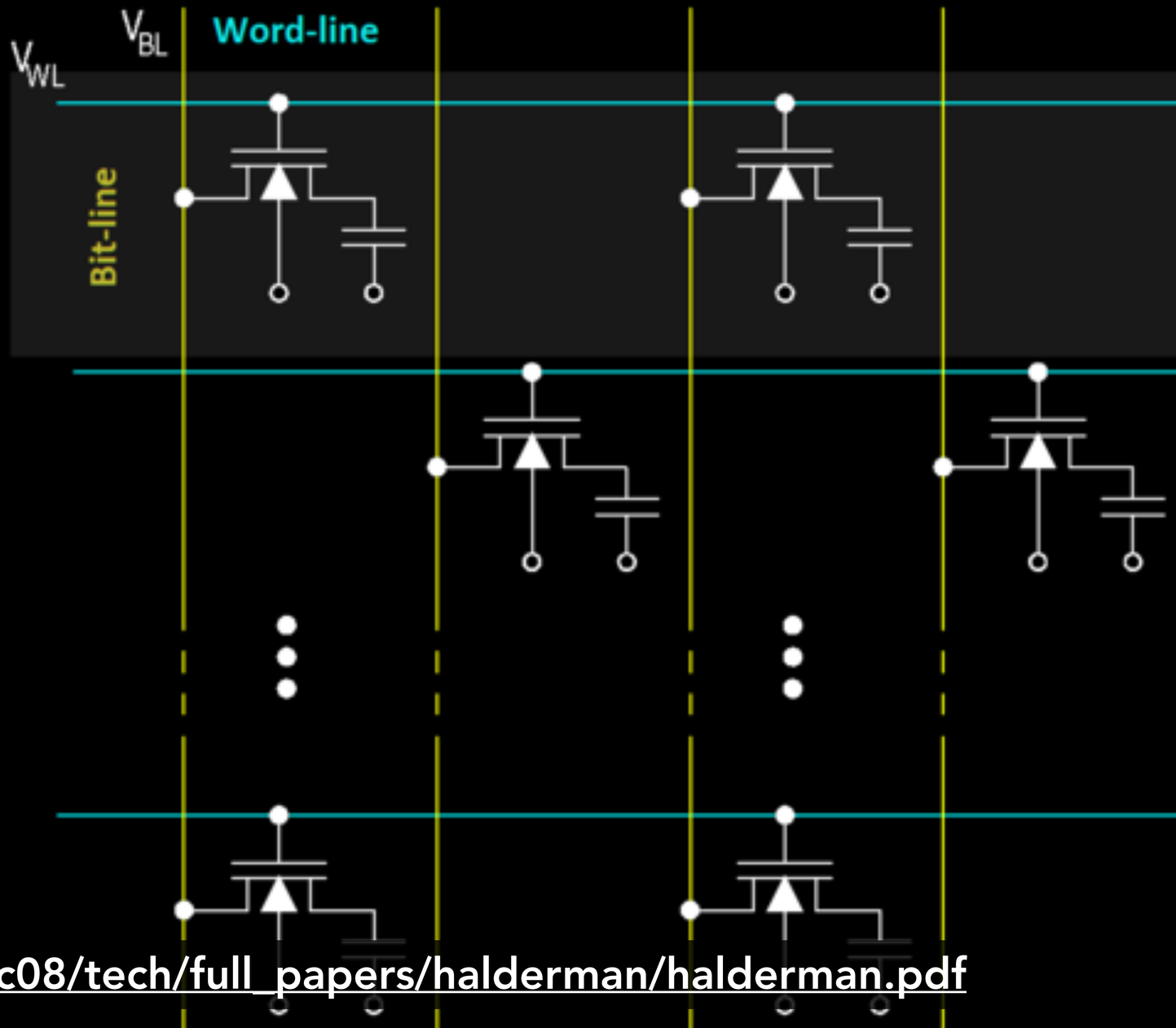
fault injection :: temperature



www.usenix.org/legacy/event/sec08/tech/full_papers/halderman/halderman.pdf

fault injection :: temperature





www.usenix.org/legacy/event/sec08/tech/full_papers/halderman/halderman.pdf

sound

sound

—

audible

(meaning, to most humans)

side channel :: sound



people.eecs.berkeley.edu/~tygar/papers/Keyboard_Acoustic_Emanations_Revisited/TISSEC.pdf

sound

—

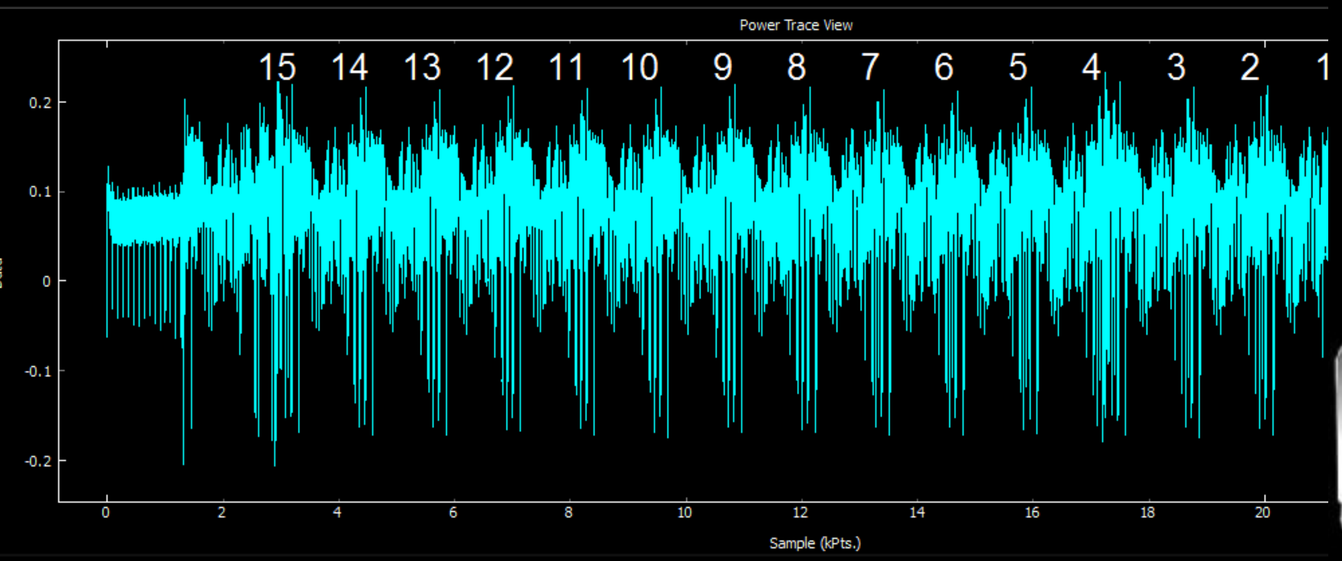
ultrasound

ultra- from Latin

“beyond” or “on the far side of"

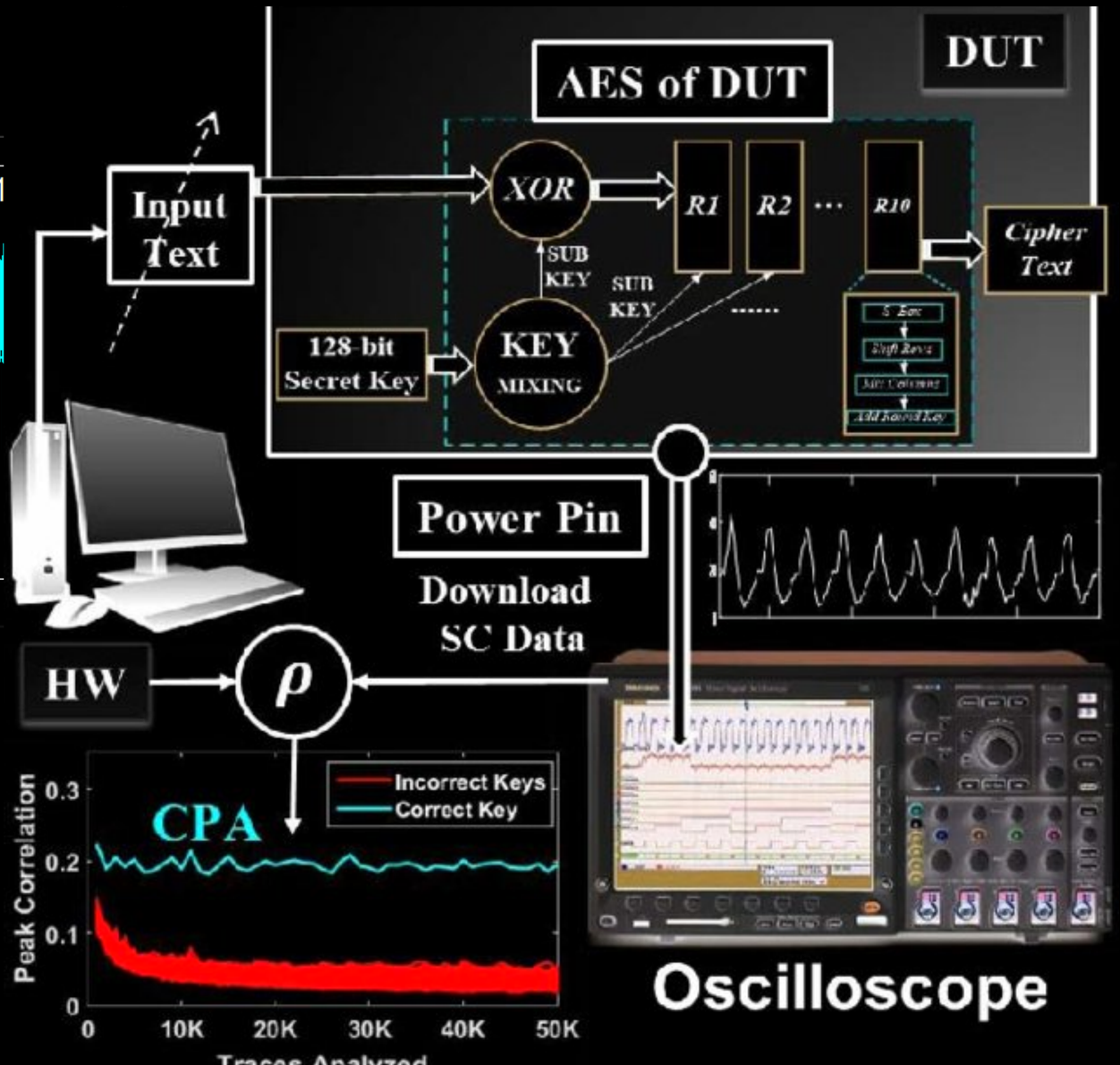


cs.tau.ac.il/~tromer/acoustic



wiki.newae.com/V3:Tutorial_B11_Breaking_RSA

ieeexplore.ieee.org/document/8351968



fault injection :: ultrasound

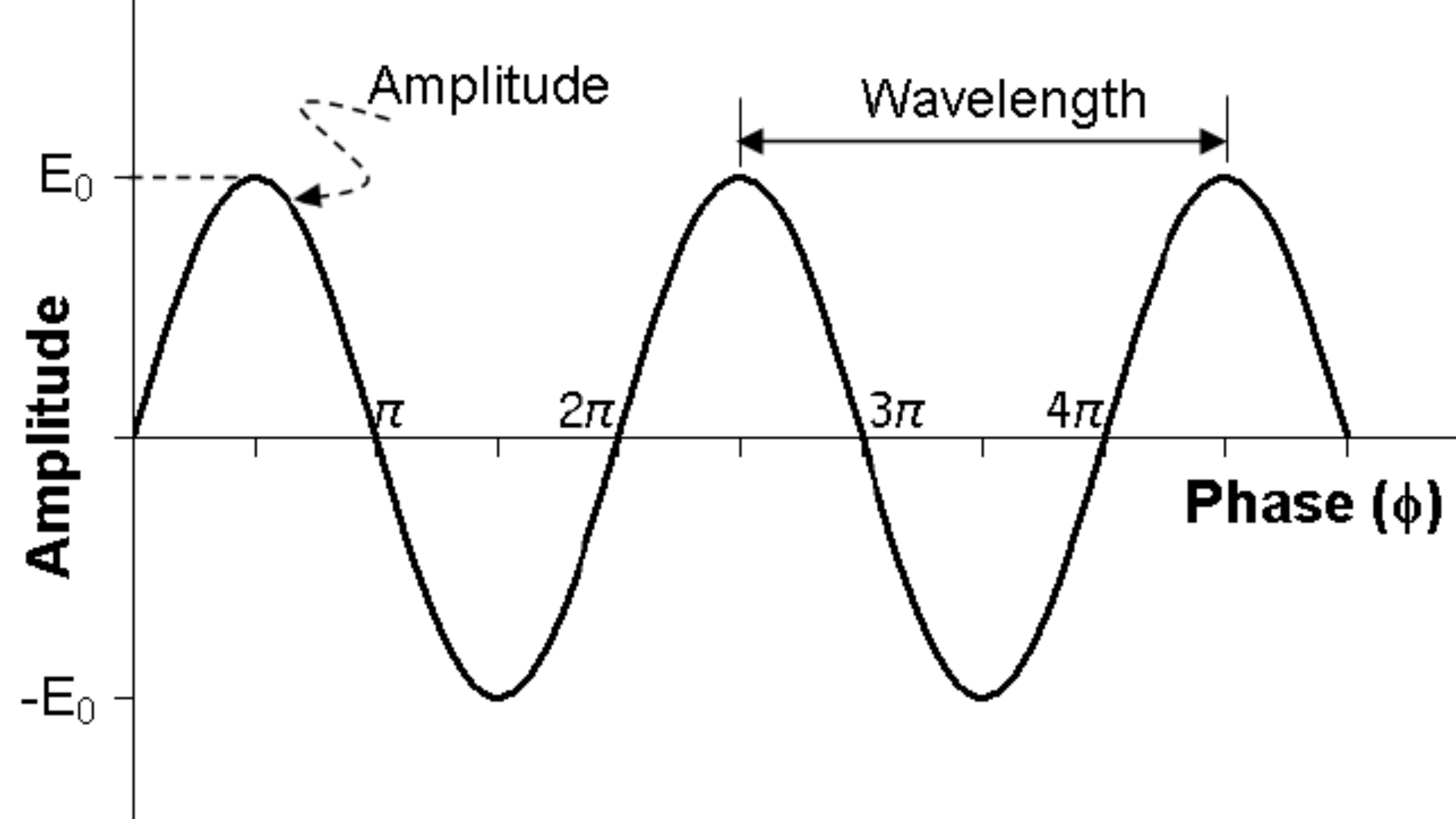


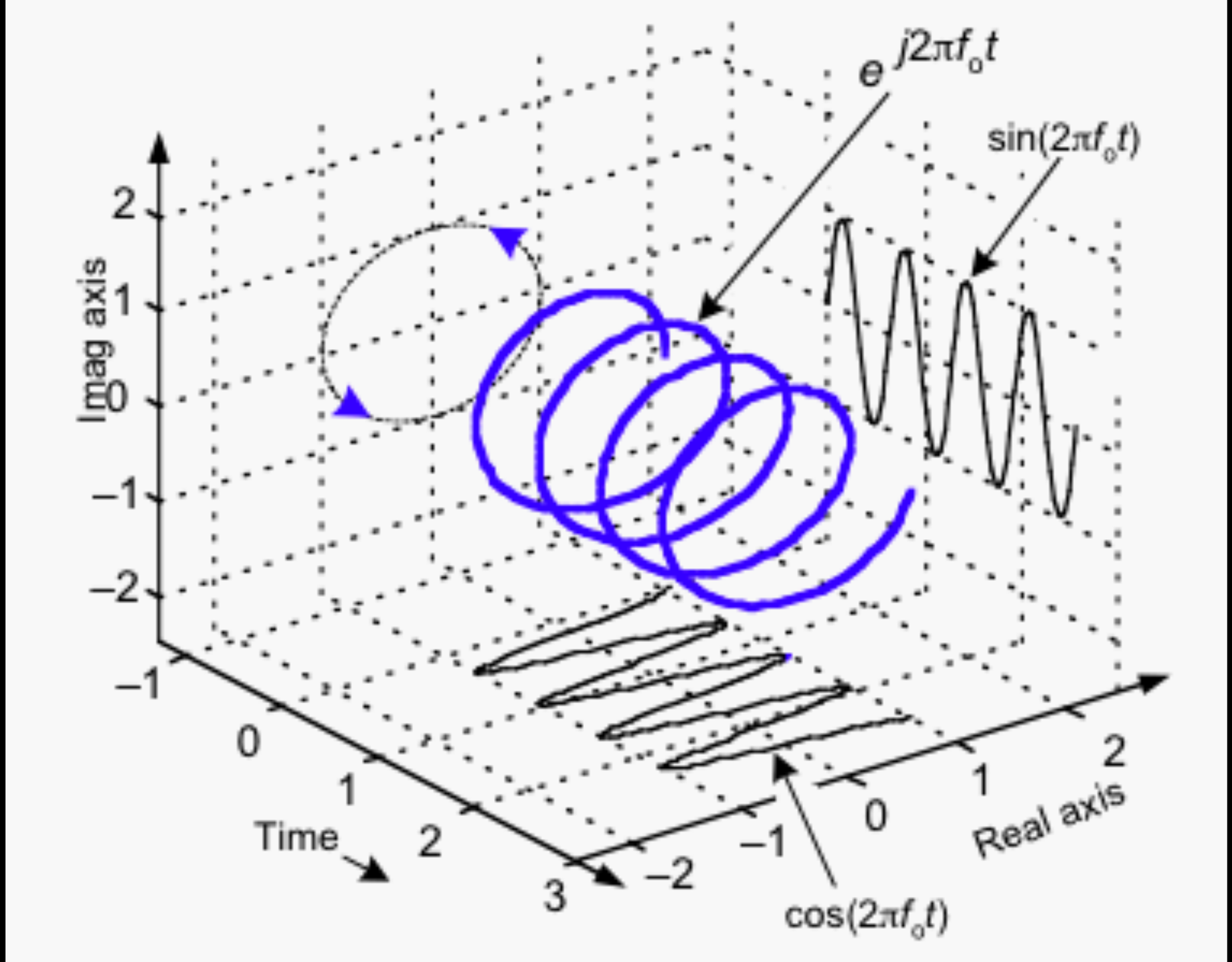
www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-son-updated.pdf

waves



youtube.com/watch?v=Iuv6hY6zsd0 (/Veritasium)


Amplitude
Wavelength
E_0
$-E_0$
Amplitude
π
2π
3π
4π
Phase (ϕ)


$e^{j2\pi f_o t}$
$\sin(2\pi f_o t)$
Imag axis
2
1
0
–1
–2
–1
0
1
2
3
Time
–2
–1
0
1
2
Real axis
$\cos(2\pi f_o t)$

light + sound

—

laser microphone

Leon Theremin



Lev Termen demonstrating the theremin, December 1927

Born	Lev Sergeyevich Termen 27 August [O.S. 15 August] 1896 Saint Petersburg, Russian Empire
Died	3 November 1993 (aged 97) Moscow, Russia
Occupation(s)	Engineer, physicist
Known for	Theremin, The Thing

Leon Theremin



Lev Termen demonstrating the theremin, December 1927

Born	Lev Sergeyevich Termen 27 August [O.S. 15 August] 1896 Saint Petersburg, Russian Empire
Died	3 November 1993 (aged 97) Moscow, Russia
Occupation(s)	Engineer, physicist
Known for	Theremin, The Thing

Theremin



Leon Theremin



Lev Termen demonstrating the theremin, December 1927

Born	Lev Sergeyevich Termen 27 August [O.S. 15 August] 1896 Saint Petersburg, Russian Empire
Died	3 November 1993 (aged 97) Moscow, Russia
Occupation(s)	Engineer, physicist
Known for	Theremin, The Thing

k g b

Leon Theremin



Lev Termen demonstrating the theremin, December 1927

Born	Lev Sergeyevich Termen 27 August [O.S. 15 August] 1896 Saint Petersburg, Russian Empire
Died	3 November 1993 (aged 97) Moscow, Russia
Occupation(s)	Engineer, physicist
Known for	Theremin, The Thing

The Thing



light + sound

—

~~laser~~ optical microphone

Sniffing Keystrokes With Lasers/Voltmeters



Side Channel Attacks Using Optical Sampling Of Mechanical Energy And Power Line Leakage

Andrea Barisani
Chief Security Engineer
<*andrea@inversepath.com*>

Daniele Bianco
Hardware Hacker
<*daniele@inversepath.com*>

INVERSE PATH
http://www.inversepath.com

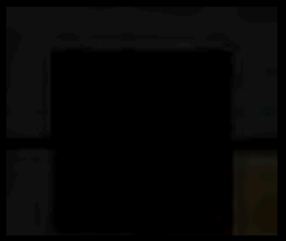
Copyright 2009 Inverse Path Ltd.

Laser Microphone Assembly



- 1 x Laser (more expensive lasers means more range)
- 1 x Photoresistor or Photodiode
- 1 x Resistor
- 1 x AA Battery
- 1 x Universal Power Adapter
- 1 x Jack Cable
- 1 x Laptop with sound card
- 2 x Tripod
- 1 x Focusing lens (for long distances)

$ 79.99



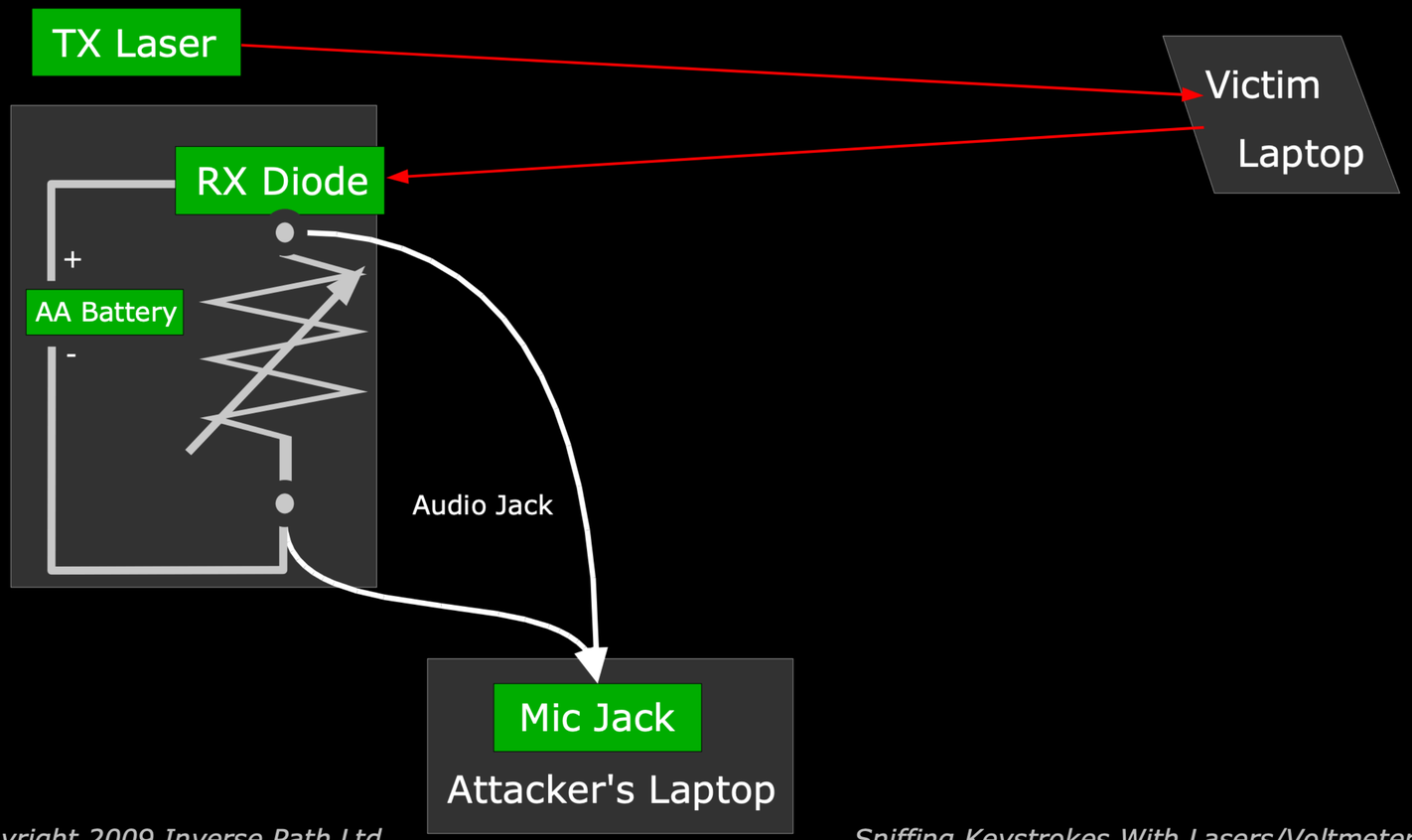
TX (The Laser)



- Class IIIR, 670 nm, <5 mW power, <2 mrad divergence (good for short range, 15-30 meters), cheap and poor laser



Diagram

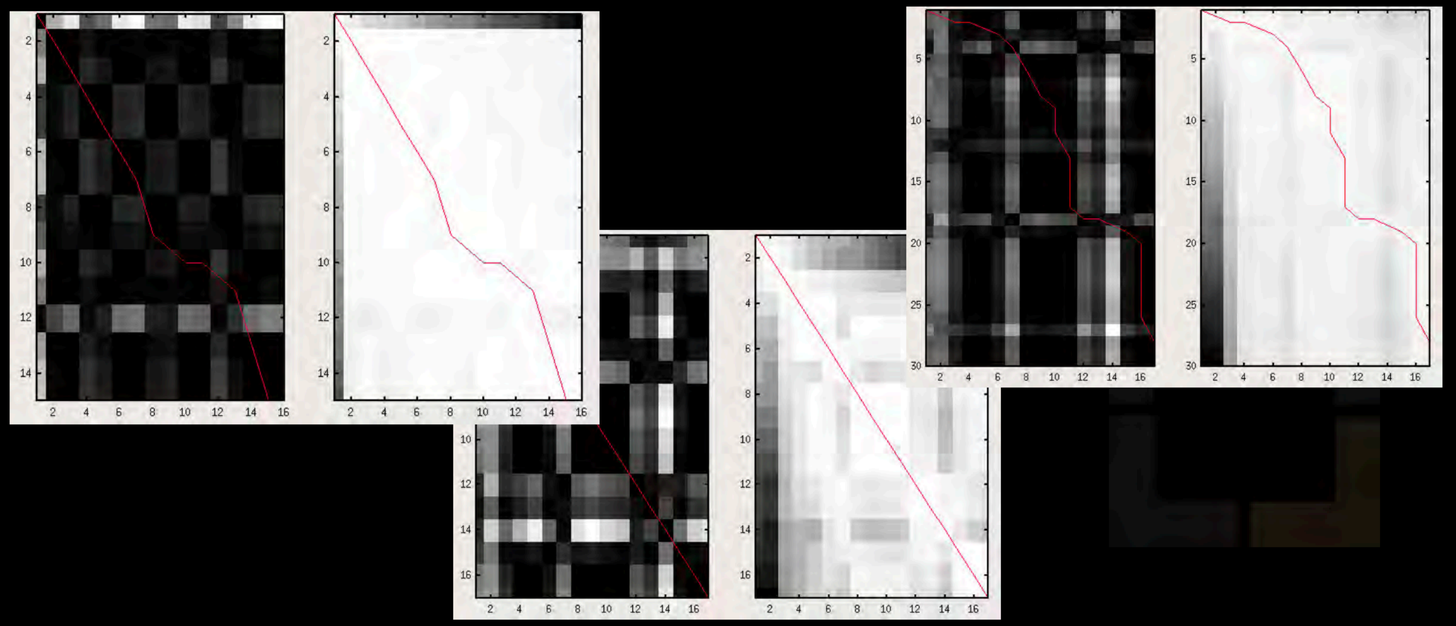


Copyright 2009 Inverse Path Ltd.

Scoring Technique



- Dynamic Time Warping (DTW) is a good technique for measuring the similarity of signals with different time/speed
- Generally applied to Audio (speech recognition) and Video



Copyright 2009 Inverse Path Ltd.

software



Georgi Gerganov
ggerganov

Unfollow | Sponsor

I like big .vimrc and I cannot lie

github.com/ggerganov/kbd-audio

kbd-audio Public

Acoustic keyboard eavesdropping

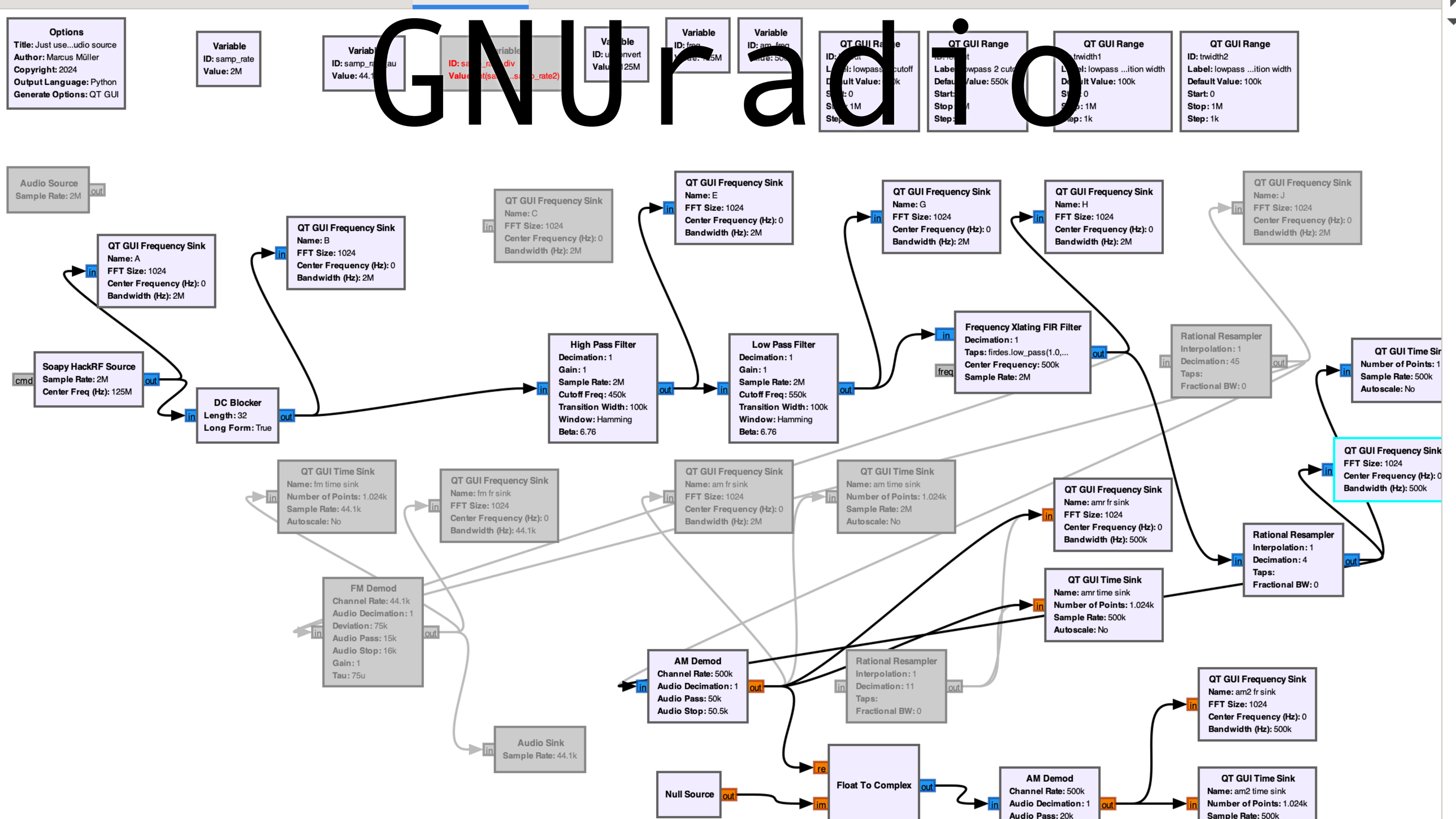
C++ 8.4k 583

- **keytap3**

  Fully automated recovery of unknown text from audio recordings.

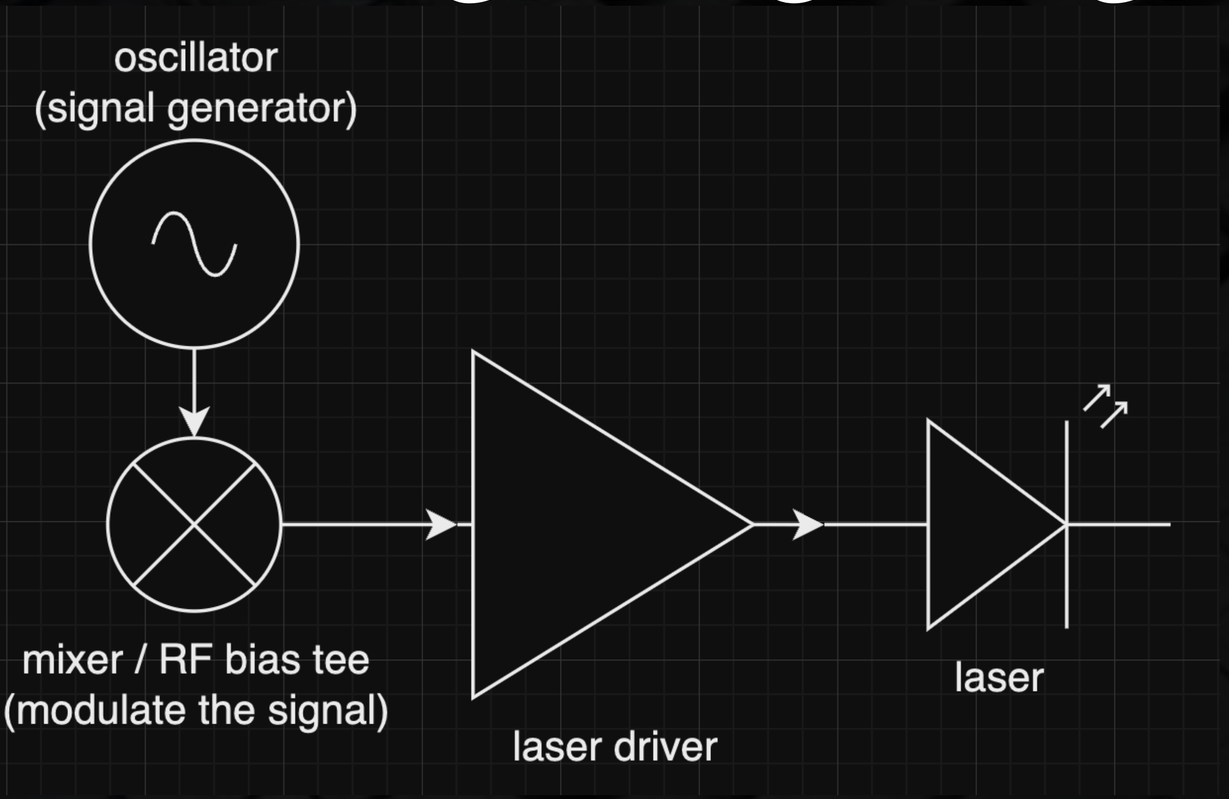
```
./keytap3 input.kbd ../data [-cN] [-CN] [-pF] [-tF] [-FN] [-fN]
```

Online demo: https://keytap3.ggerganov.com

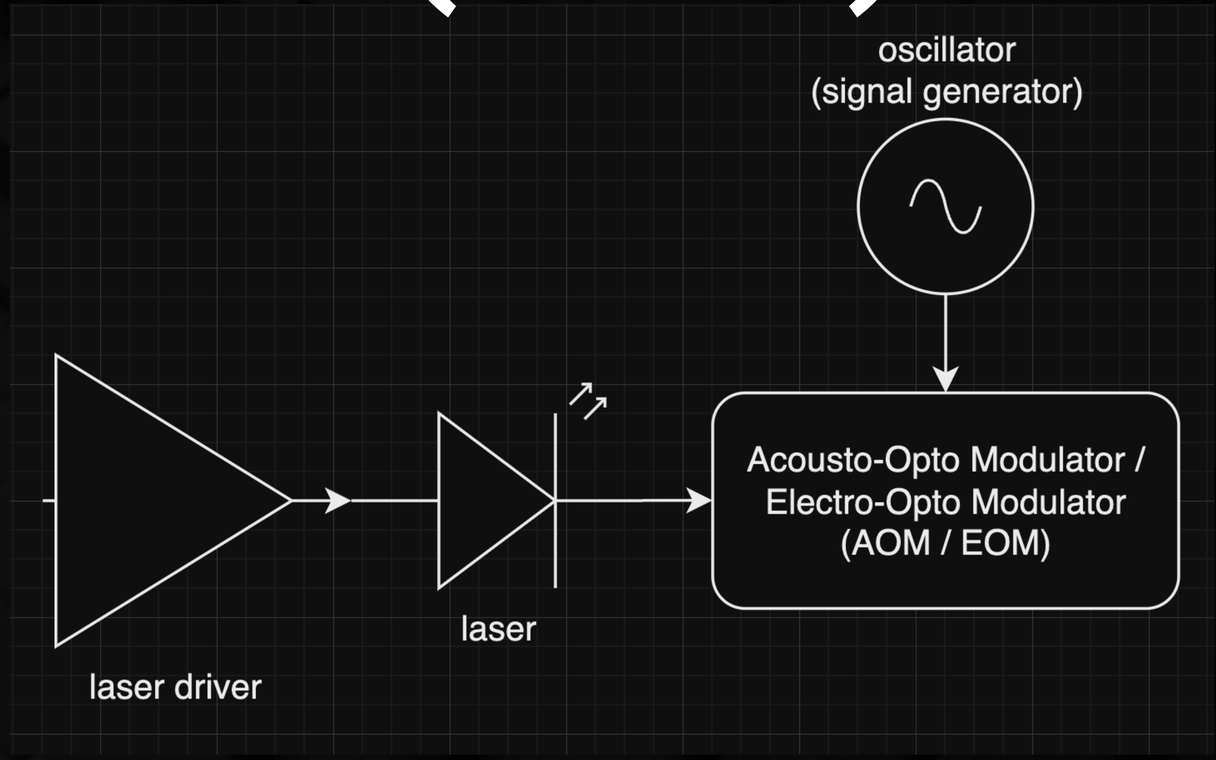

GNUradio
Options
Title: Just use...udio source
Author: Marcus Müller
Copyright: 2024
Output Language: Python
Generate Options: QT GUI
Variable
ID: samp_rate
Value: 2M
Variable
ID: freq
Variable
ID: am_freq
QT GUI Range
QT GUI Range
Label: lowpass 2 cutoff
Value: 550k
QT GUI Range
ID: trwidth1
Label: lowpass ...ition width
Default Value: 100k
QT GUI Range
ID: trwidth2
Label: lowpass ...ition width
Default Value: 100k
Start: 0
Stop: 1M
Step: 1k
Audio Source
Sample Rate: 2M
QT GUI Frequency Sink
Name: A
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 2M
QT GUI Frequency Sink
Name: B
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 2M
QT GUI Frequency Sink
Name: C
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 2M
QT GUI Frequency Sink
Name: E
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 2M
QT GUI Frequency Sink
Name: G
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 2M
QT GUI Frequency Sink
Name: H
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 2M
QT GUI Frequency Sink
Name: J
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 2M
Soapy HackRF Source
Sample Rate: 2M
Center Freq (Hz): 125M
DC Blocker
Length: 32
Long Form: True
High Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 2M
Cutoff Freq: 450k
Transition Width: 100k
Window: Hamming
Beta: 6.76
Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 2M
Cutoff Freq: 550k
Transition Width: 100k
Window: Hamming
Beta: 6.76
Frequency Xlating FIR Filter
Decimation: 1
Taps: firdes.low_pass(1.0,...
Center Frequency: 500k
Sample Rate: 2M
Rational Resampler
Interpolation: 1
Decimation: 45
Taps:
Fractional BW: 0
QT GUI Time Sir
Number of Points: 1
Sample Rate: 500k
Autoscale: No
QT GUI Frequency Sink
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 500k
QT GUI Time Sink
Name: fm time sink
Number of Points: 1.024k
Sample Rate: 44.1k
Autoscale: No
QT GUI Frequency Sink
Name: fm fr sink
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 44.1k
QT GUI Frequency Sink
Name: am fr sink
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 2M
QT GUI Time Sink
Name: am time sink
Number of Points: 1.024k
Sample Rate: 2M
Autoscale: No
QT GUI Frequency Sink
Name: amr fr sink
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 500k
Rational Resampler
Interpolation: 1
Decimation: 4
Taps:
Fractional BW: 0
QT GUI Time Sink
Name: amr time sink
Number of Points: 1.024k
Sample Rate: 500k
Autoscale: No
FM Demod
Channel Rate: 44.1k
Audio Decimation: 1
Deviation: 75k
Audio Pass: 15k
Audio Stop: 16k
Gain: 1
Tau: 75u
AM Demod
Channel Rate: 500k
Audio Decimation: 1
Audio Pass: 50k
Audio Stop: 50.5k
Rational Resampler
Interpolation: 1
Decimation: 11
Taps:
Fractional BW: 0
Audio Sink
Sample Rate: 44.1k
Null Source
Float To Complex
AM Demod
Channel Rate: 500k
Audio Decimation: 1
Audio Pass: 20k
QT GUI Frequency Sink
Name: am2 fr sink
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 500k
QT GUI Time Sink
Name: am2 time sink
Number of Points: 1.024k
Sample Rate: 500k

hardware

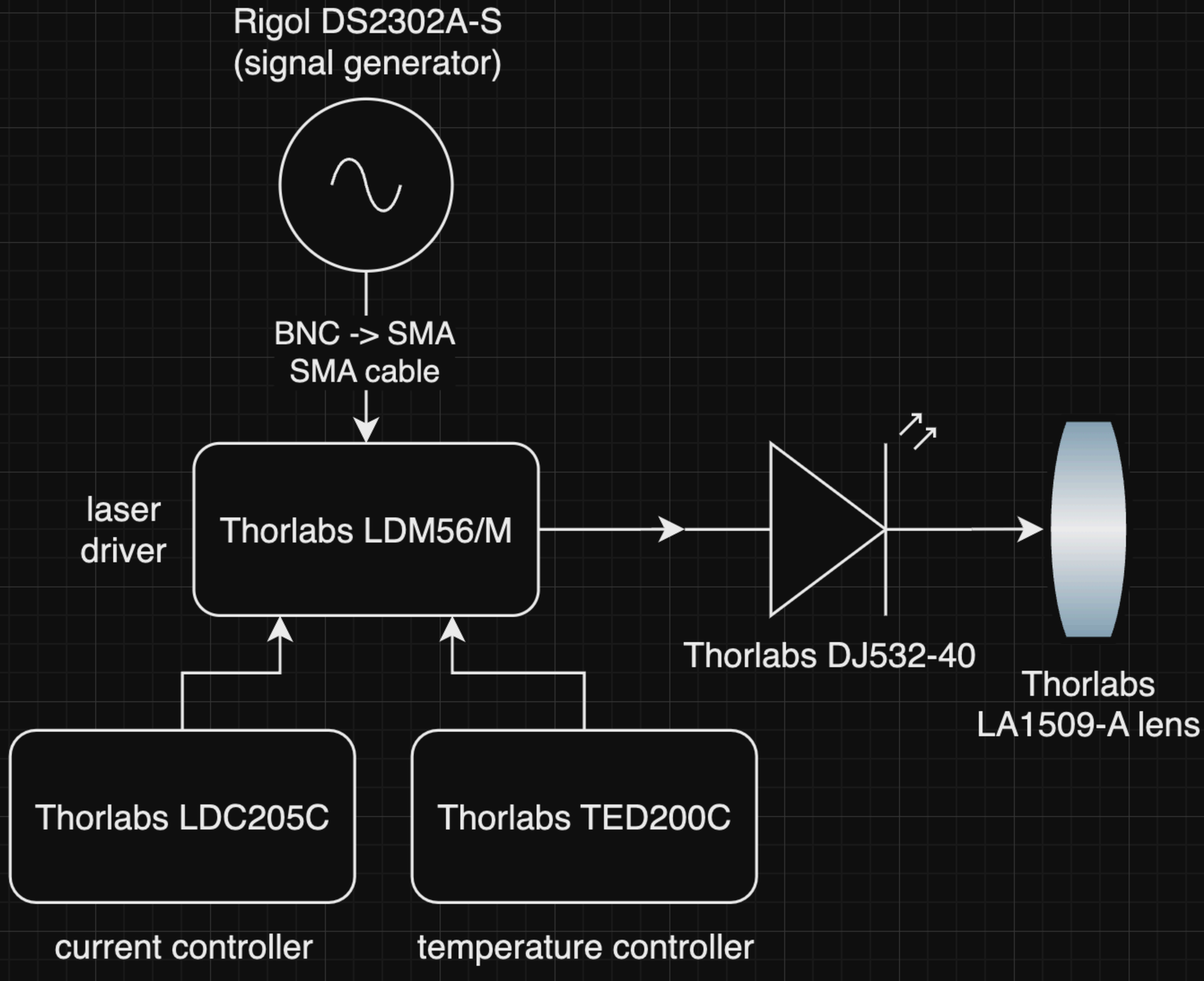
hardware (tx)



or

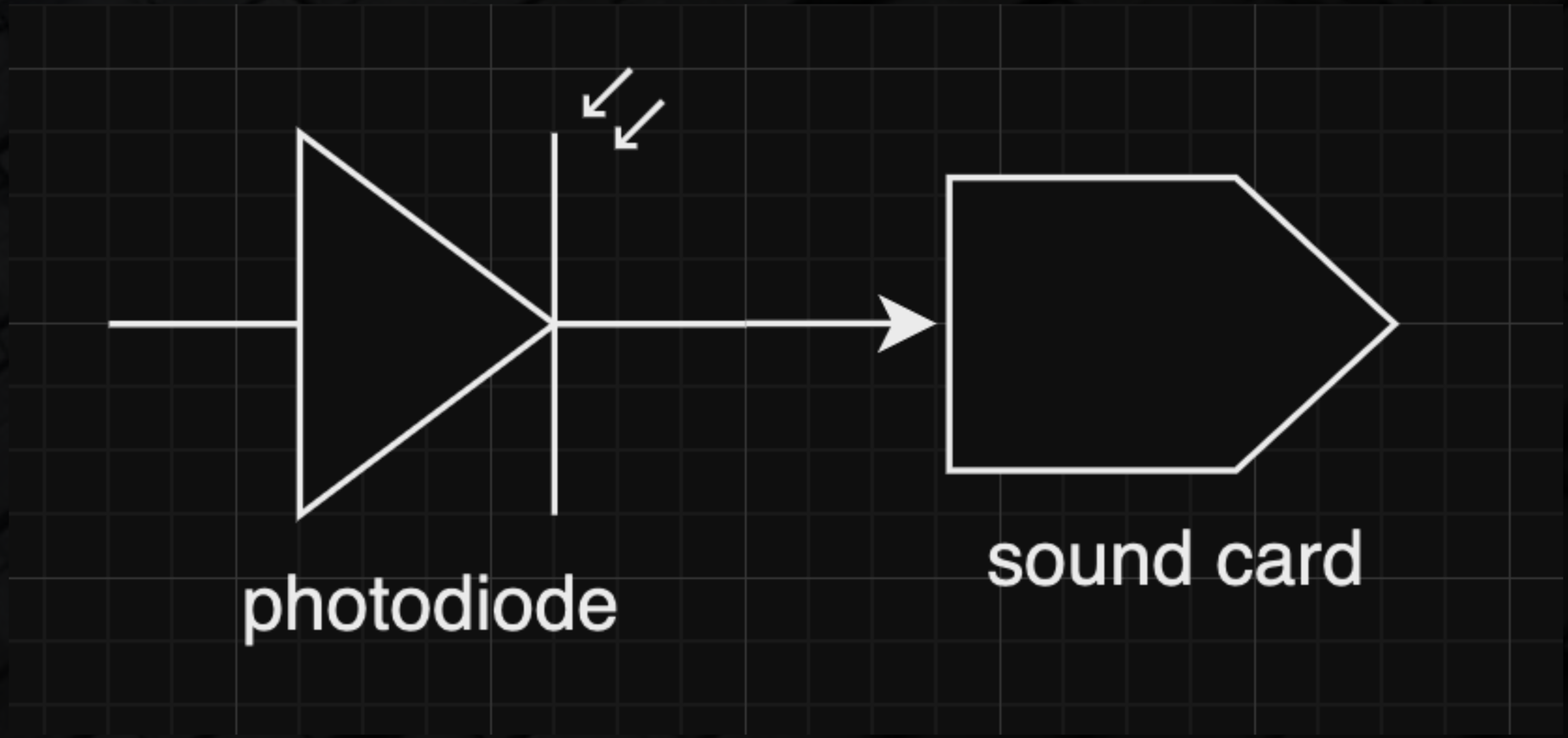


our tx side


Rigol DS2302A-S
(signal generator)
BNC -> SMA
SMA cable
laser
driver
Thorlabs LDM56/M
Thorlabs DJ532-40
Thorlabs
LA1509-A lens
Thorlabs LDC205C
Thorlabs TED200C
current controller
temperature controller

hardware (rx)

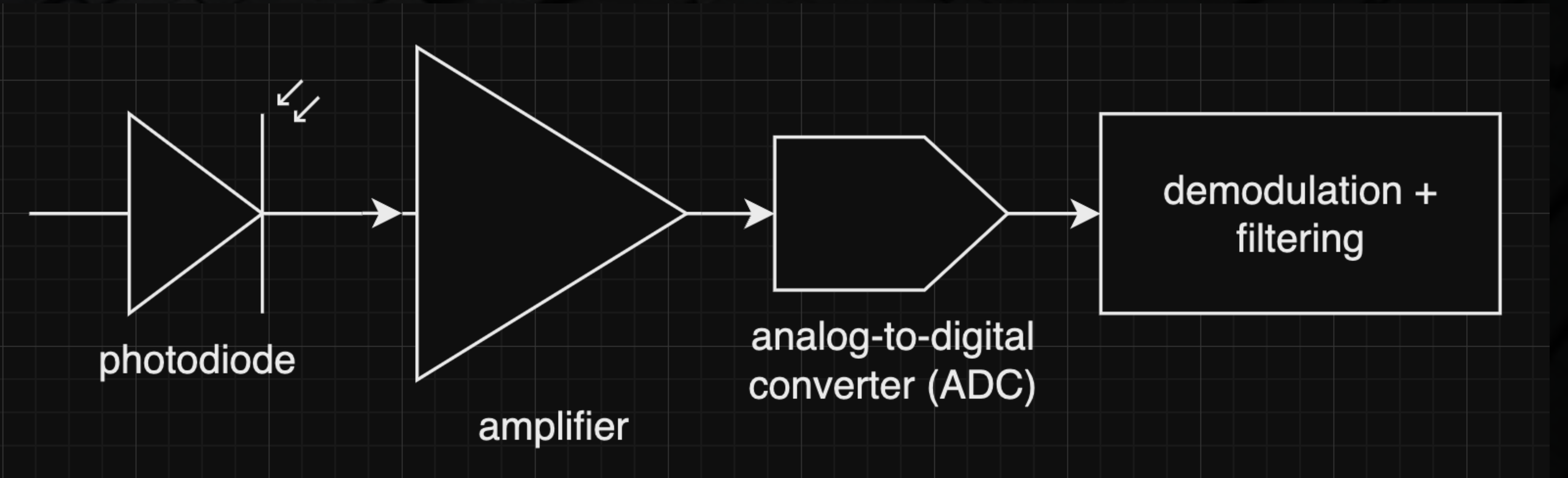
typical setup



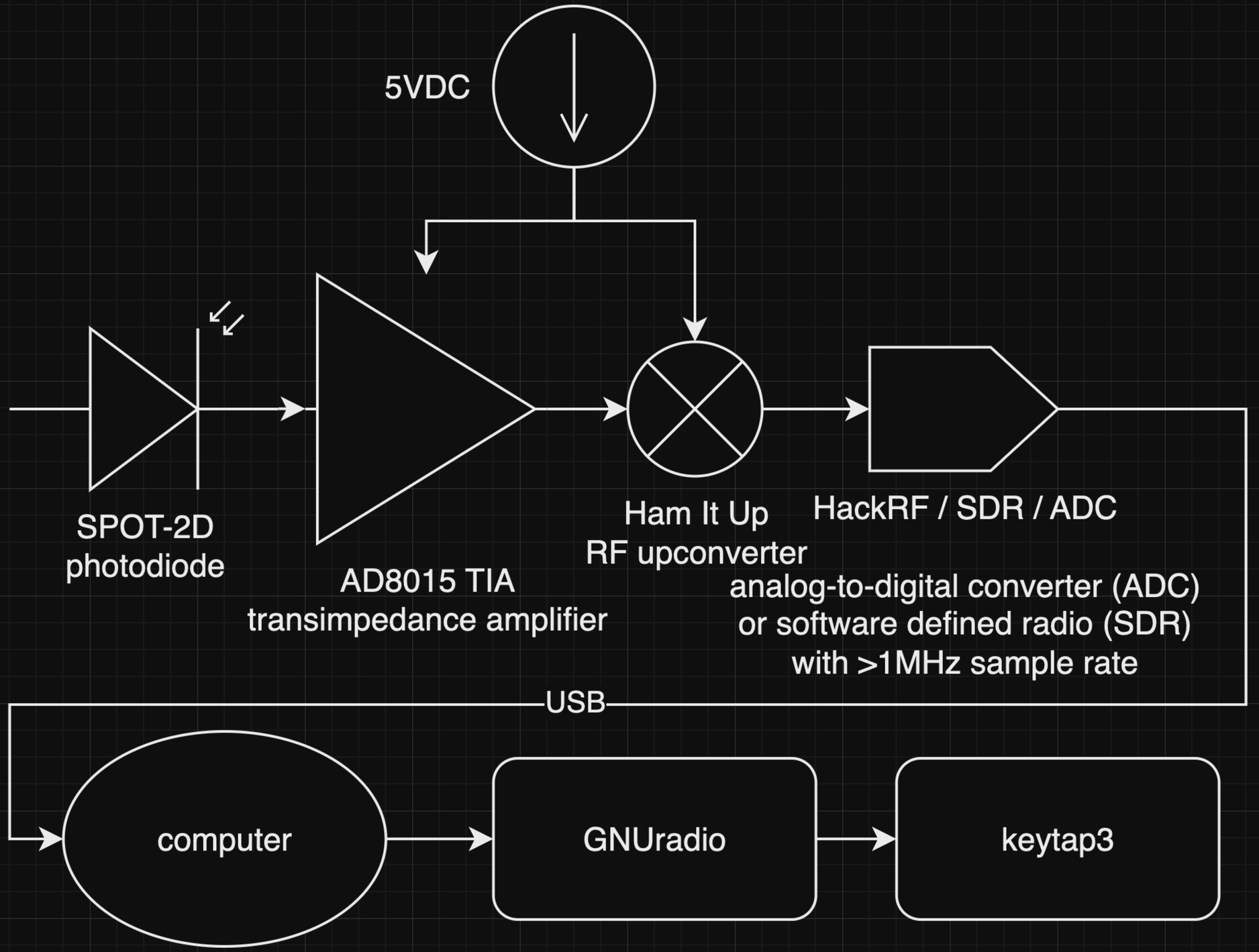
hardware (rx)

our setup

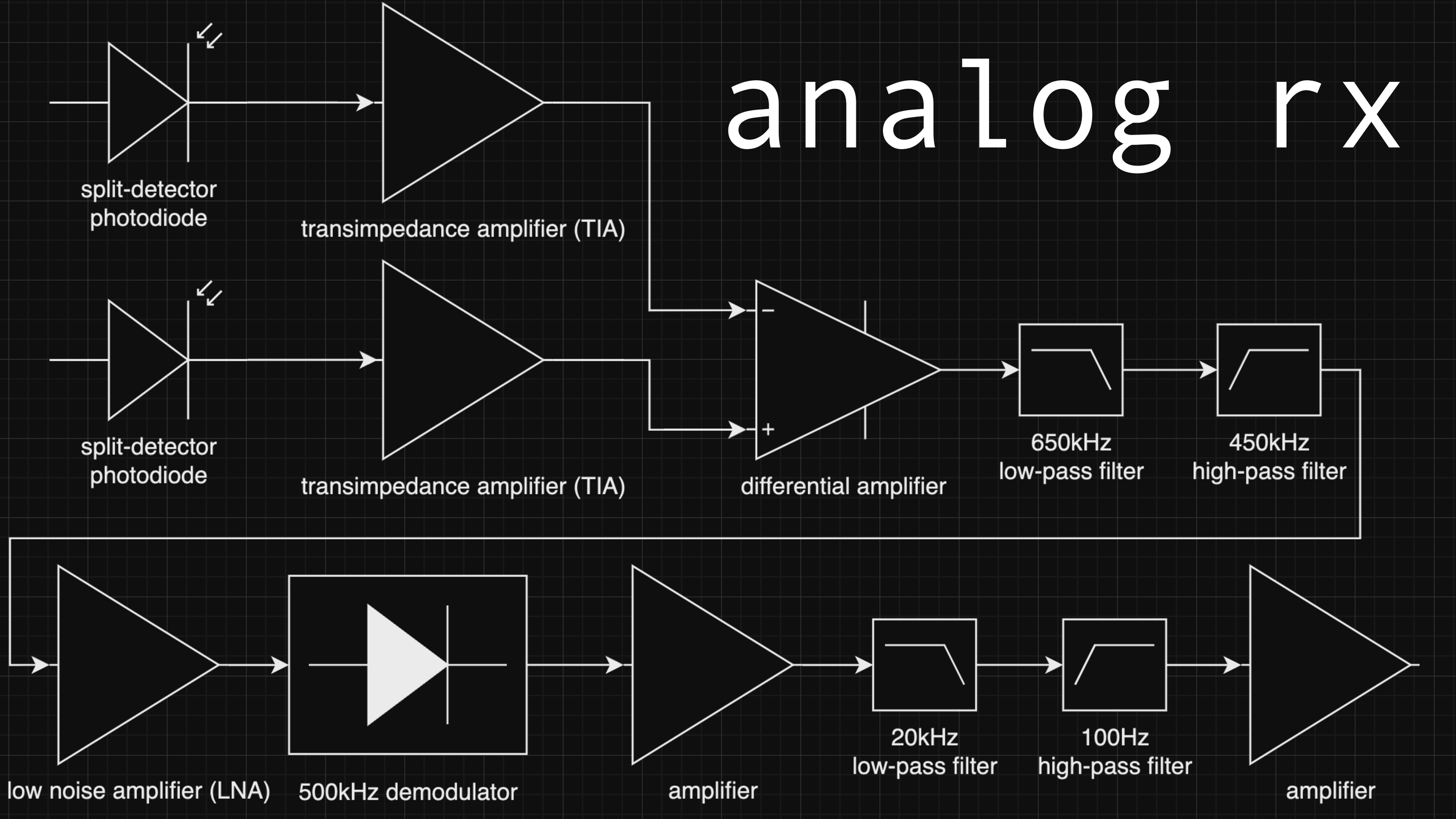
don't use sound card!



our rx side


5VDC
SPOT-2D
photodiode
AD8015 TIA
transimpedance amplifier
Ham It Up
RF upconverter
HackRF / SDR / ADC
analog-to-digital converter (ADC)
or software defined radio (SDR)
with >1MHz sample rate
USB
computer
GNUradio
keytap3

analog rx


split-detector photodiode
transimpedance amplifier (TIA)
split-detector photodiode
transimpedance amplifier (TIA)
differential amplifier
650kHz low-pass filter
450kHz high-pass filter
low noise amplifier (LNA)
500kHz demodulator
amplifier
20kHz low-pass filter
100Hz high-pass filter
amplifier

hardware (tx)

(simpler/cheaper components can be used!)

- Laser diode
  - IR: Thorlabs HL8338MG (803nm, 50mW, 5.6mm LD)
  - Green: Thorlabs DJ532-40 (532nm, 40mW, 9mm DPSS)
- Laser driver (w/TE-cooling + RF bias tee): Thorlabs LDM56/M
  - Diode mount: Thorlabs LDM56DJ
- Current controller: Thorlabs LDC205C
- Temperature controller: Thorlabs TED200C
- Signal generator: Rigol DS2302A-S

hardware (rx)

(using SDR)

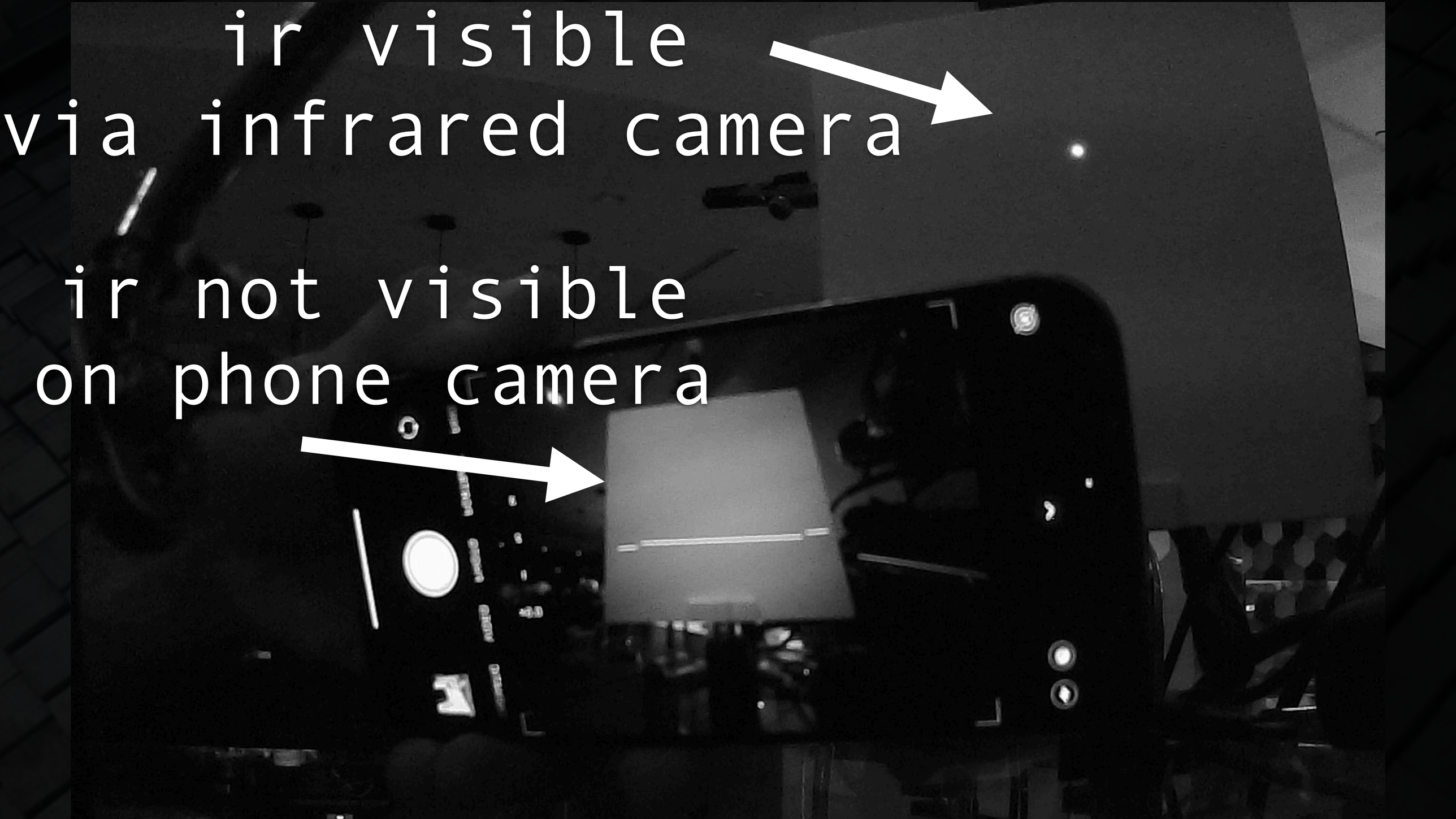
- UV+Vis+IR camera: XNiteUSB2S-M
- Split-cell photodiode: SPOT-2D
- Transimpedance amps (TIA): AD8015
- HF upconverter: Ham It Up v1.3
- SDR: HackRF / USRP B210 (RTL-SDR would likely work)

hardware (rx)

(alternatively using analog/scope ADC)

- Split-cell photodiode: SPOT-2D
- Transimpedance amplifiers (TIA): Analog Devices AD8015
- RF Filters: Mini Circuits
- Filters + AC Coupling: Rigol DS2302A-S (from TX side) -> output to USB
- Demodulator: 1N4148+0.0022uF cap+5kΩ resistor

tx
infrared

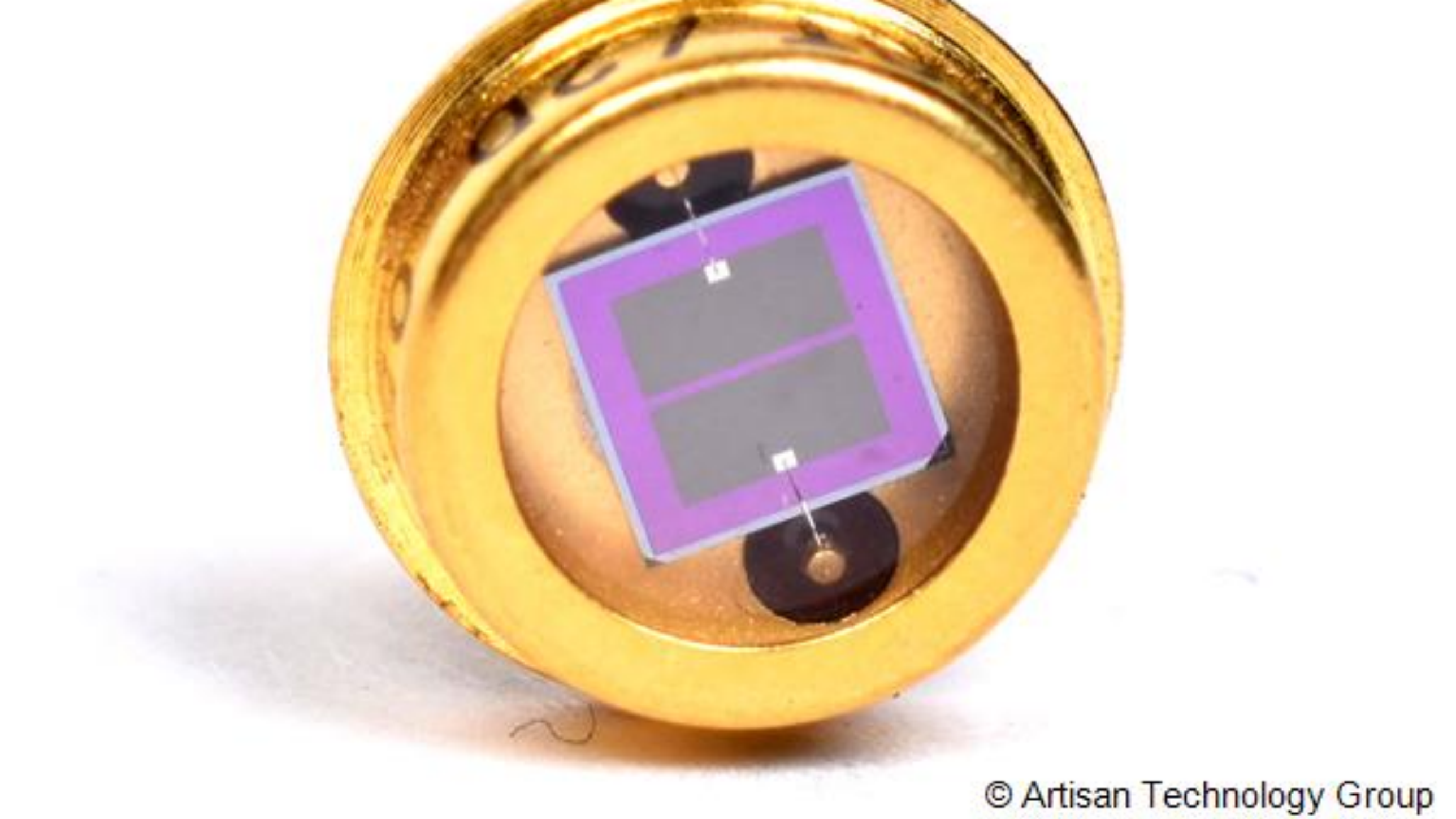

ir visible
via infrared camera
ir not visible
on phone camera

tx RF modulation

rx split cell photodiode

—

common mode noise rejection



© Artisan Technology Group

rx transimpedance amplifier — current -> voltage

rx RF bandpass filtering

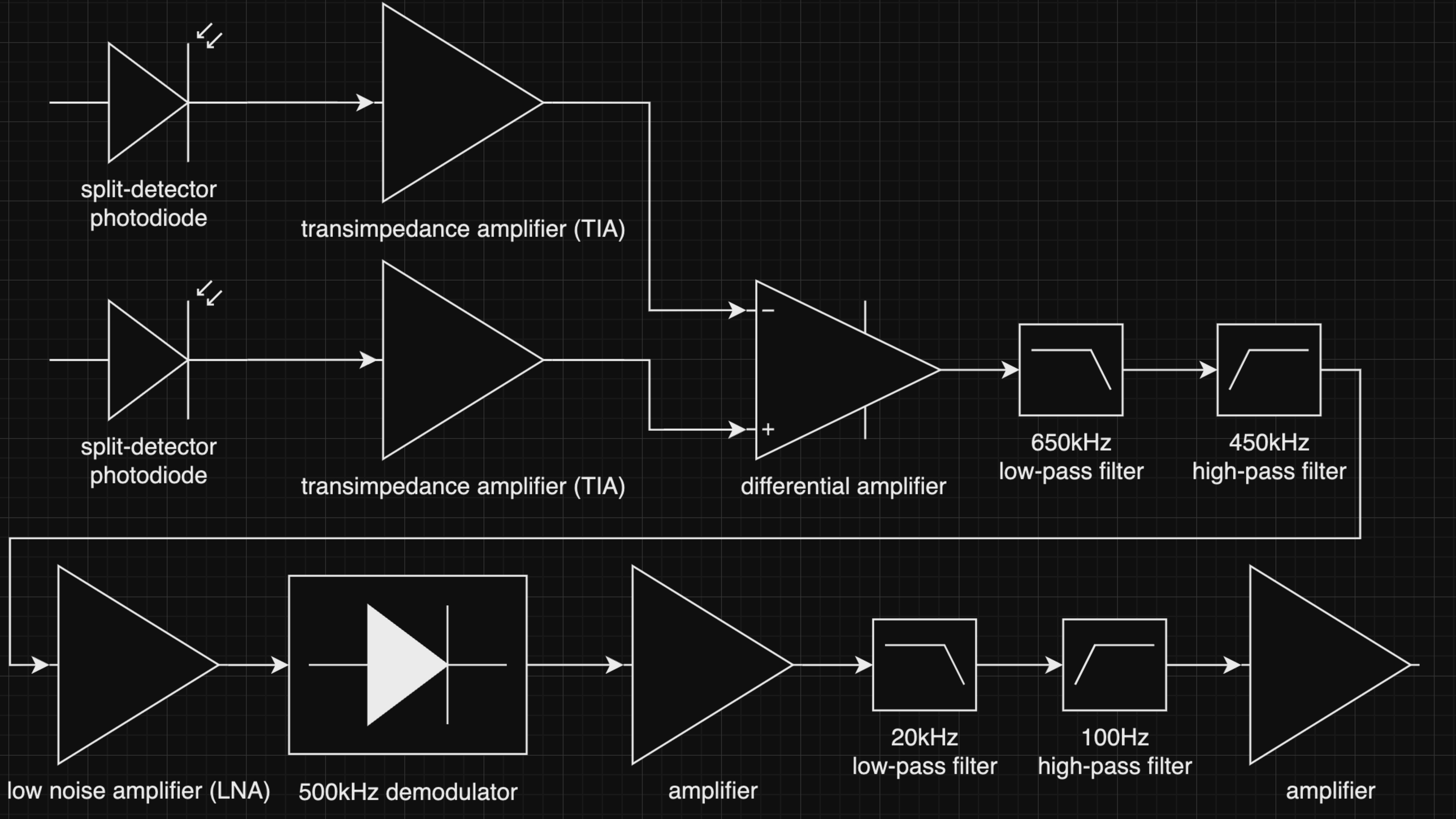
rx RF demodulation

—

envelope detector / synchronous demodulation

rx audible-range bandpass filtering

rx low noise amplification


split-detector photodiode
transimpedance amplifier (TIA)
split-detector photodiode
transimpedance amplifier (TIA)
differential amplifier
650kHz low-pass filter
450kHz high-pass filter
low noise amplifier (LNA)
500kHz demodulator
amplifier
20kHz low-pass filter
100Hz high-pass filter
amplifier


RIGOL
Counter
78.469 kHz
I2C
Read:12
Data:R
Data:I
Data:G
1 2.00V +3.60V
2 2.00V -400mV
3 1.32V +633mV
4 100mV 0.00V
GI
GII
LA

rigolna.com

interferometer

actual:

hello and welcome to the laser microphone test where we are now converting light to sounds well actually signal as we never technically hear the signal as sound since it does not get directly recorded or played back

keytap3:

hhello_and_welcome_to_thheplaser_microohone_test_where_we_are_now_converting_lightto_sounds_awelll_acitualllysignasl_aos_we_netheir_techniciallytreast_the_sigaal_as_sound_isince_int_ddoes_not_get_aged_intly_recolrded_or_llayedf [-5.654   -0.235]

ground truth

latest @ samy.pl/dc32

Optical Espionage

(and other ways to exploit physics)

@samykamkar
samy.pl