Université de Rennes

IETR

Remote data extraction through retroreflector hardware implants

Pierre Granier (PhD student)
François Sarrazin (Junior Professor Chair)
Team eWAVES

{pierre.granier, francois.sarrazin}@univ-rennes.fr

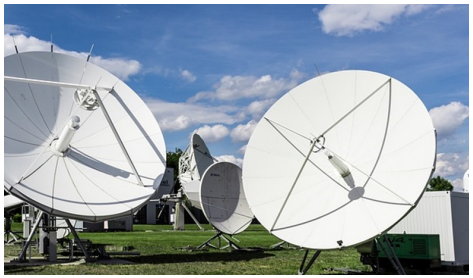
CentraleSupélec
rennes
INSA RENNES
Nantes Université
Université de Rennes

18/12/2024

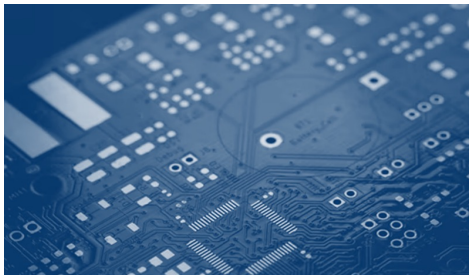
www.ietr.fr

IETR Laboratory – UMR CNRS 6164

Institut d'Electronique et des Technologies du numéRique (360 people / half PhD)

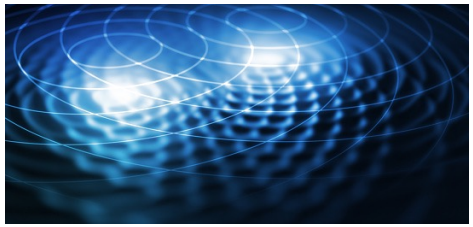


Antennas and complex radiating systems

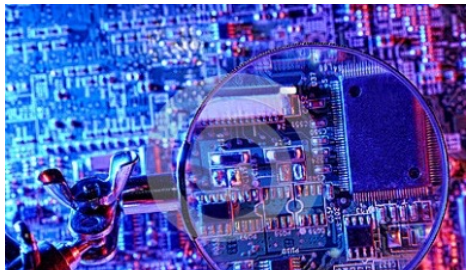


Micro-technologies, Materials and sensors

Hardware Cybersecurity

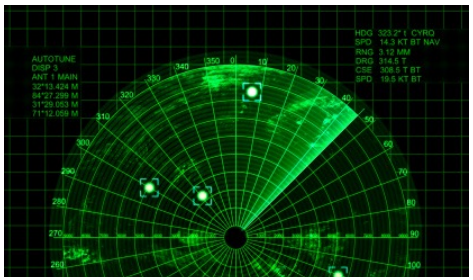


Complex interactions of waves with matter and living organisms



Smart embedded, reliable and flexible intelligents systems

Communication systems, digital networks and equipment



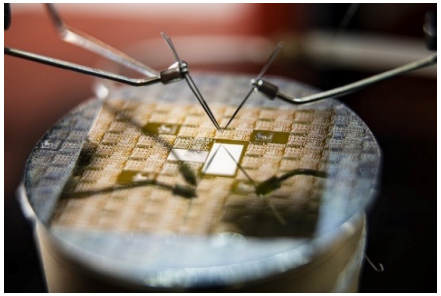
Propagation and radar technologies, detection, location

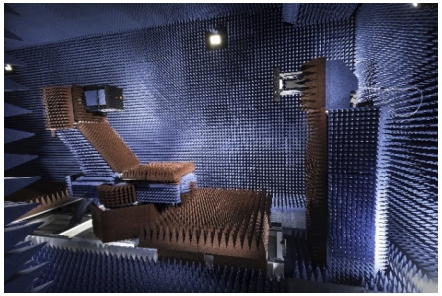
Image Processing, video codec, and artificial intelligence

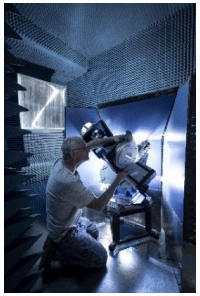
Energy systems for transition

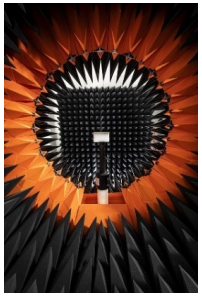
IETR Laboratory – UMR CNRS 6164

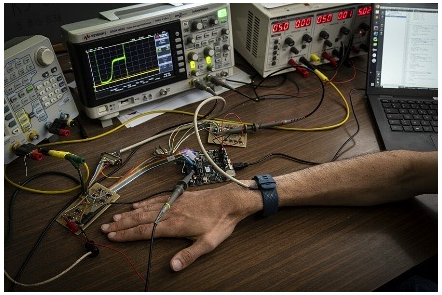
Experimental facilities

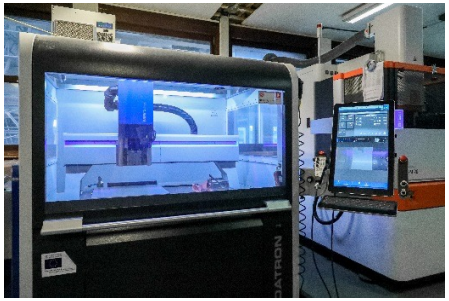












CentraleSupélec
rennes
INSA RENNES
Nantes Université
Université de Rennes

Outline

I/. Introduction to EM Cybersecurity

A bit of history

TEMPEST attack on a VGA cable

Basic concept of a Radio-Frequency Retroreflector Attack (RFRA)

II/. RFRA

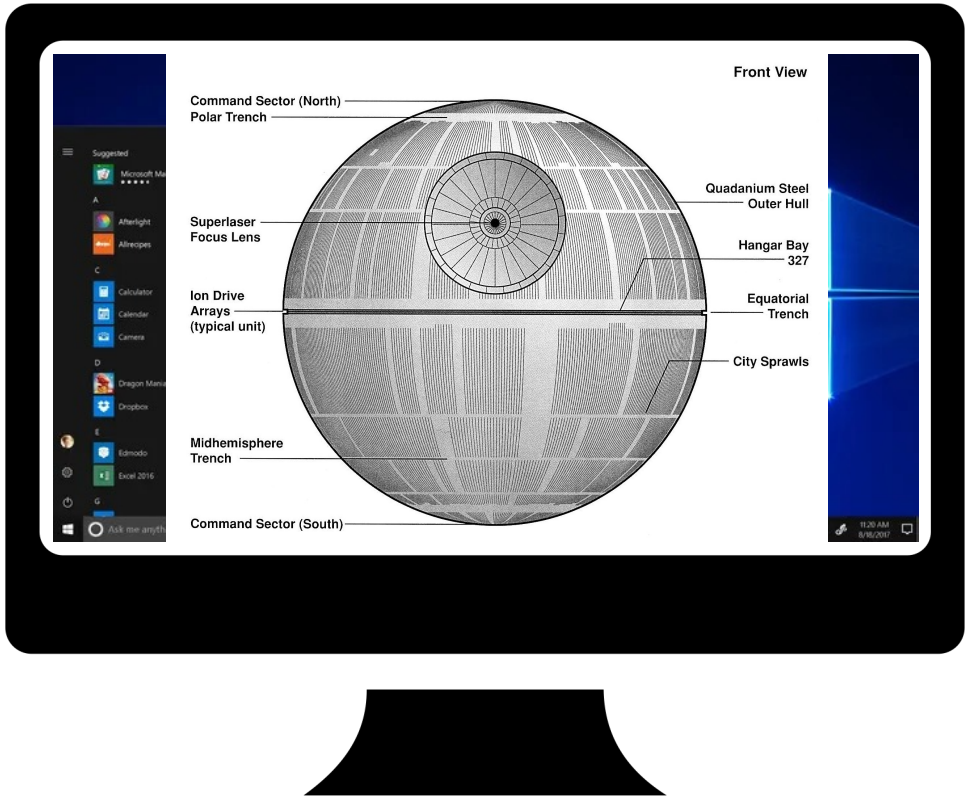
New trojan architecture

Multi trojans attacks

TEMPEST

Objective of the attack: Retrieve information displayed on a screen

Why?



How?

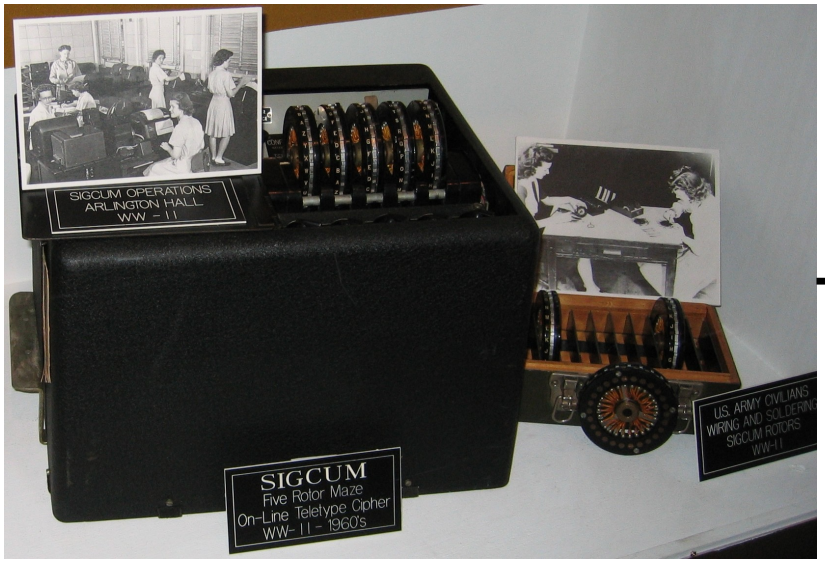
Electromagnetic eavesdropping

IETR TEMPEST

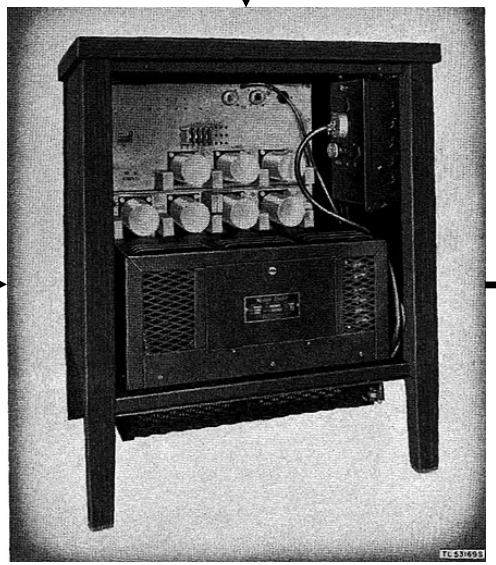
From EM Compatibility… to EM Cybersecurity

TEMPEST

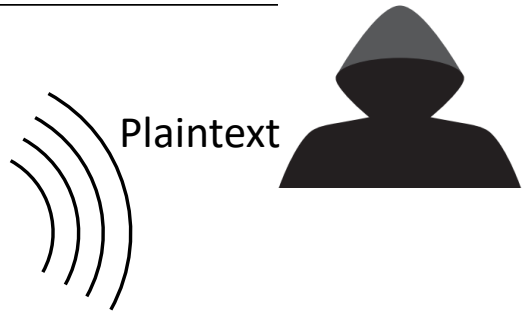
First discovery during WWII - Telegrapher



SIGCUM Rotor Cipher Machine



Mixer 131-B2 by Bell Telephone

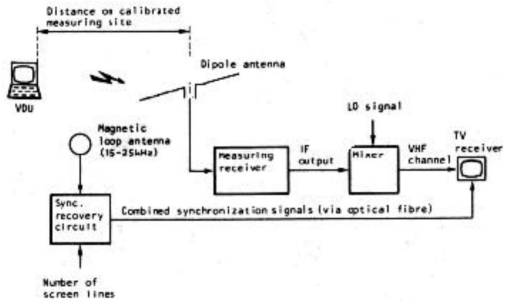


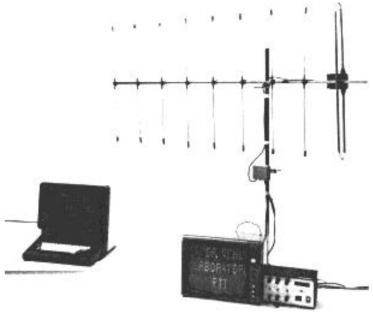
Start of the TEMPEST program by the US, includes attacks and countermeasures
TEMPEST became a standard for protection (shielding, restricted area)

IETR TEMPEST

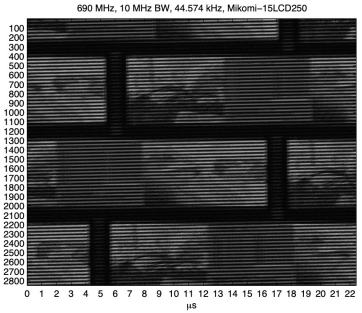
Academic works

Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?
Wim Van Eck (1985)



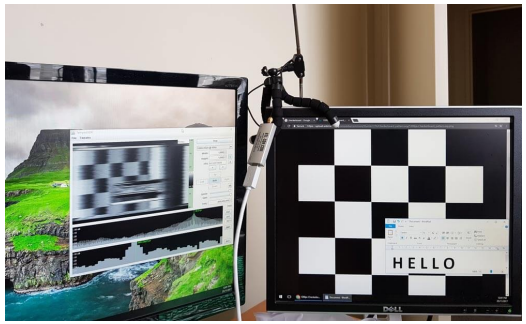


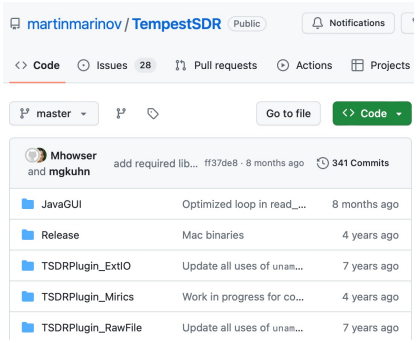
Compromising emanations: eavesdropping risks of computer displays
Markus G. Kuhn (2003)



Compromising Emanations of LCD TV Sets
Markus G. Kuhn (2013)

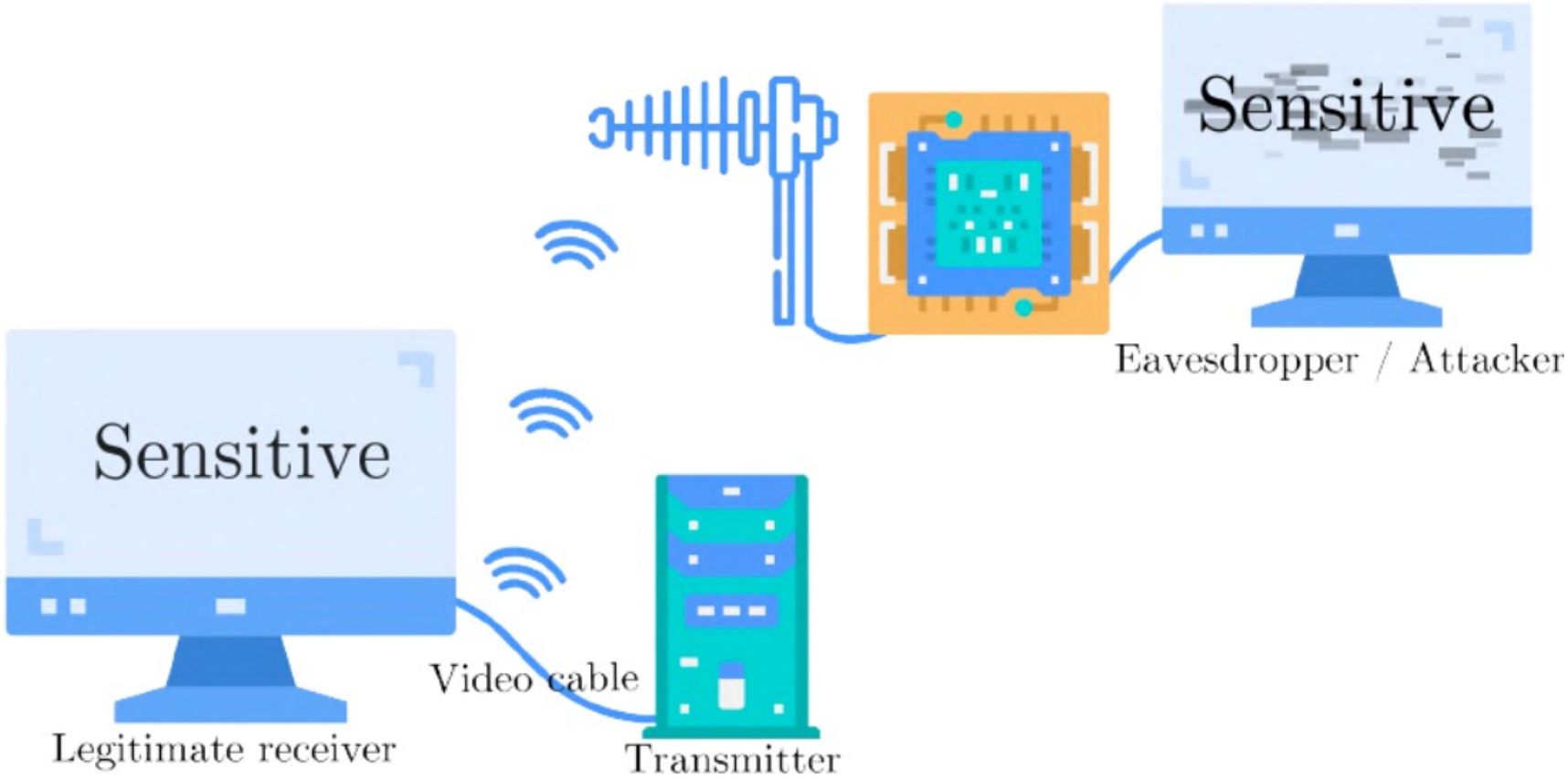
Remote video eavesdropping using a software-defined radio platform
M. Marinov (2015)





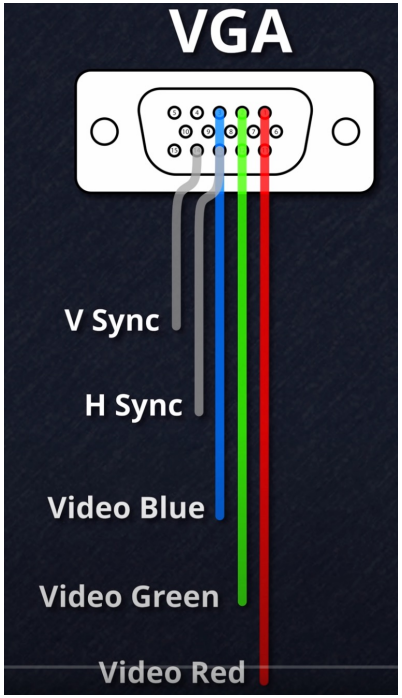
TEMPEST

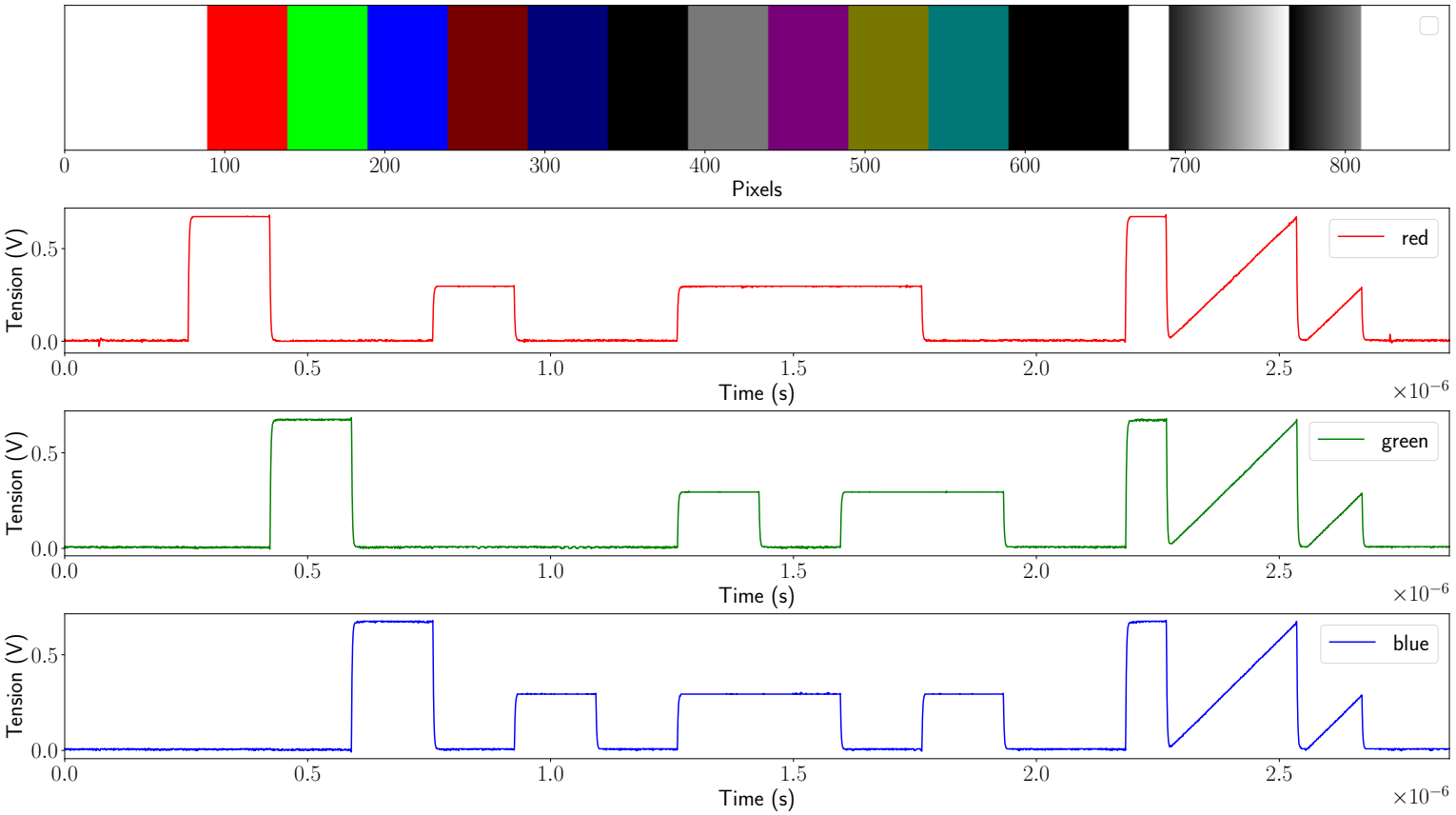
How does it work?



TEMPEST

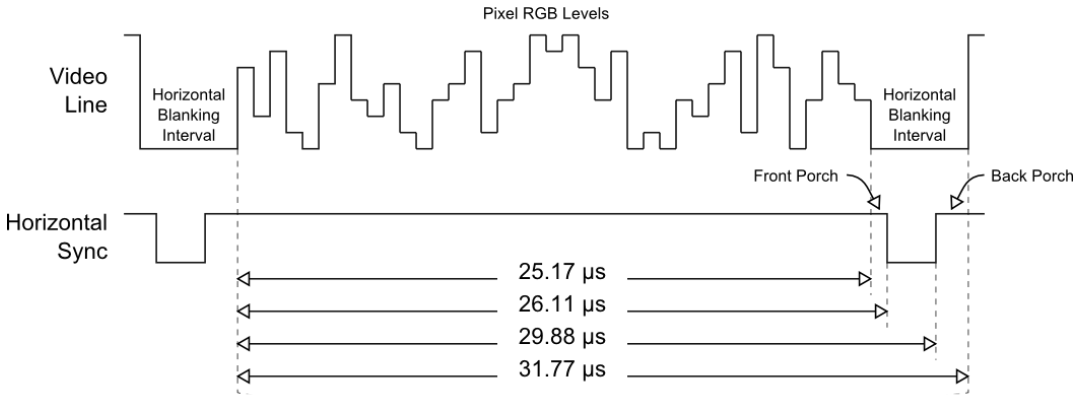
VGA protocol

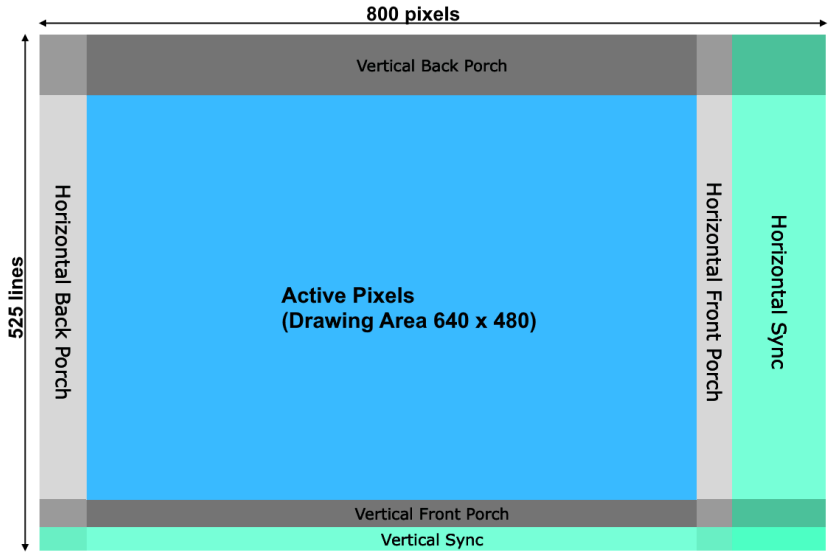




RGB signals probed with an oscilloscope

TEMPEST


Pixel RGB Levels
Video Line
Horizontal Blanking Interval
Horizontal Blanking Interval
Front Porch
Back Porch
Horizontal Sync
25.17 µs
26.11 µs
29.88 µs
31.77 µs


800 pixels
525 lines
Vertical Back Porch
Horizontal Back Porch
Active Pixels
(Drawing Area 640 x 480)
Horizontal Front Porch
Horizontal Sync
Vertical Front Porch
Vertical Sync

TEMPEST

Why does it radiate?

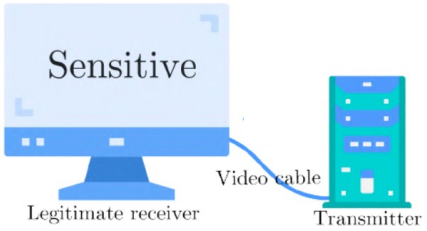
Because

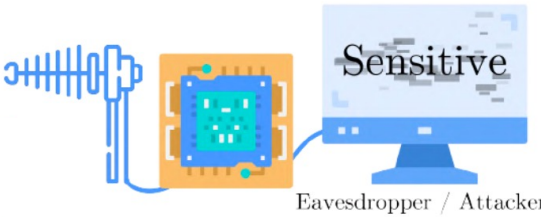
Maxwell's equations!!!

$$\mathbf{rot}\ \mathbf{H} = \mathbf{J} + \varepsilon \frac{\partial \mathbf{E}}{\partial t} \qquad \mathbf{rot}\ \mathbf{E} = -\mu \frac{\partial \mathbf{H}}{\partial t}$$

$$\mathbf{J} \propto \cos(\omega t) \longrightarrow \mathbf{H} \propto \cos(\omega t) \quad \mathbf{E} \propto \cos(\omega t) \longrightarrow \mathbf{J} \propto \cos(\omega t)$$

Progressive self-sustained electromagnetic wave





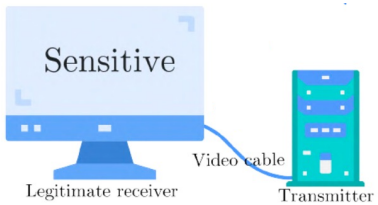
- Twisted pair
- Differential mode (D+/D-)
- Shielding

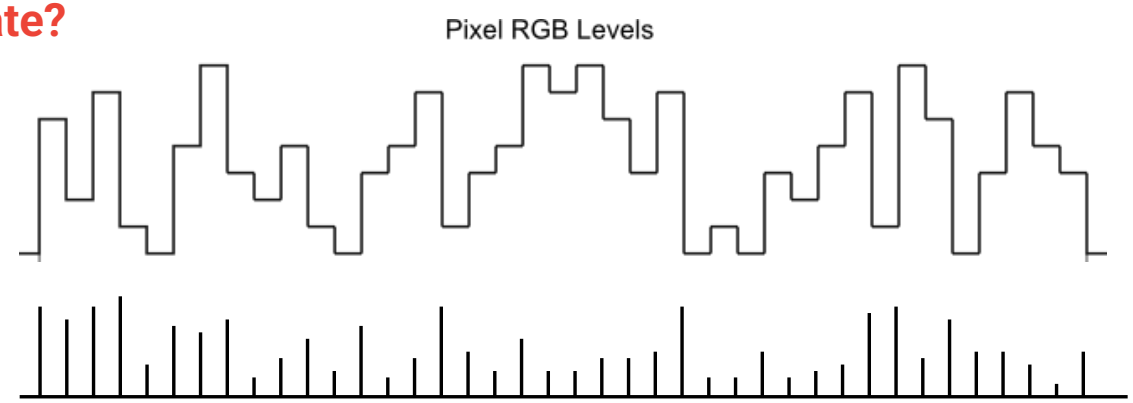
Damaged Braided Shielding

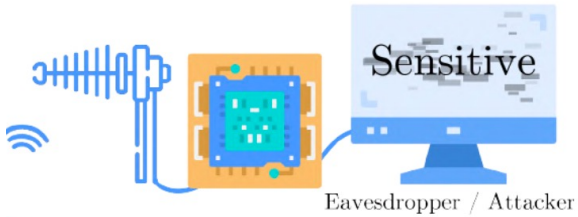
Unshielded connectors

TEMPEST

When does it radiate?





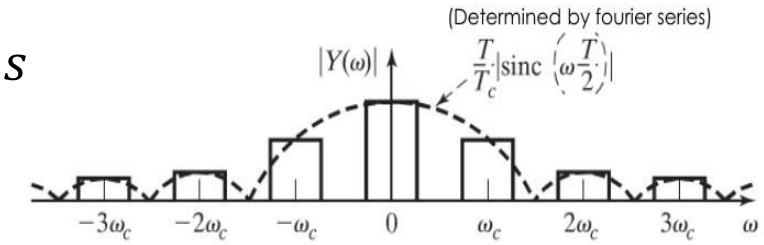


Looks like Pulse Amplitude Modulation (PAM)!

At what career frequency?

$$Pixel_{clock} = \frac{1}{T_{pixel}} = nb_{line} * nb_{col} * fps$$

640*480 @60 Hz → **25 MHz**
1920*1080 @60 Hz → **173 MHz**



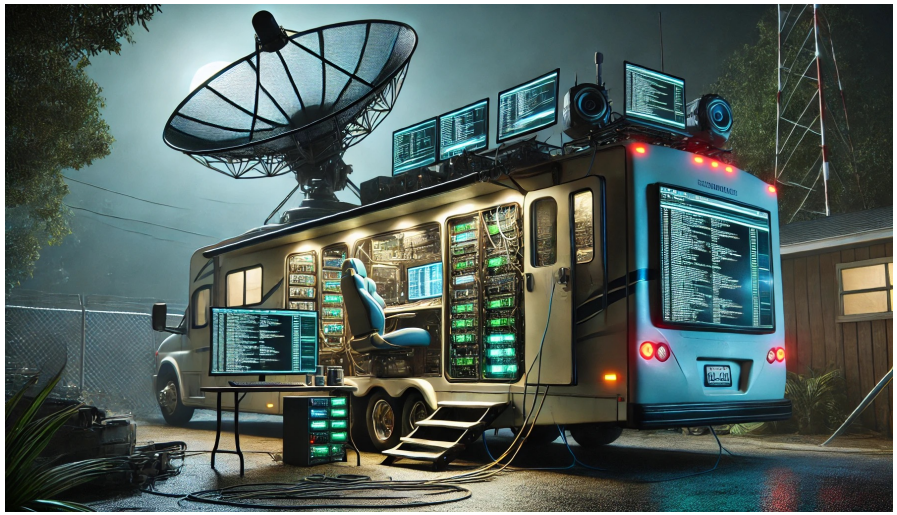
PAM Spectrum

$$F_{leak} = n * Pixel_{clock}$$

Tradeoff!

TEMPEST

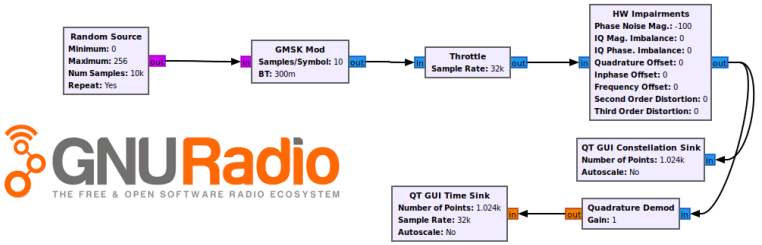
How to capture the EM leaks?



What people think

What it actually is

Cheap SDR platforms

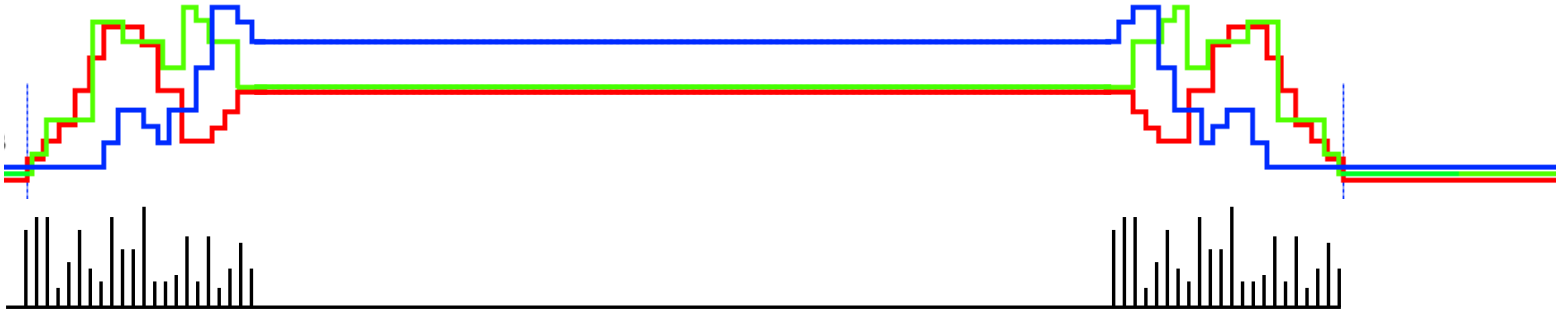


Limits of the VGA attack

Black and White

No color change -> no leaks

Unsigned

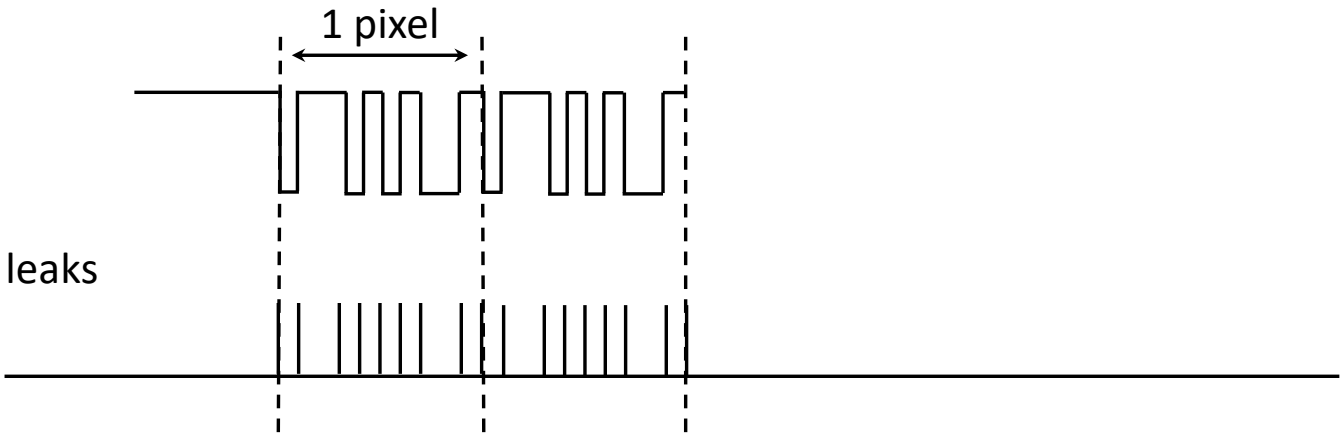


HDMI

10 bits per pixel

Sampling frequency *10

No color change -> still some leaks



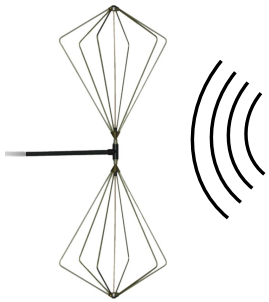
IETR TEMPEST

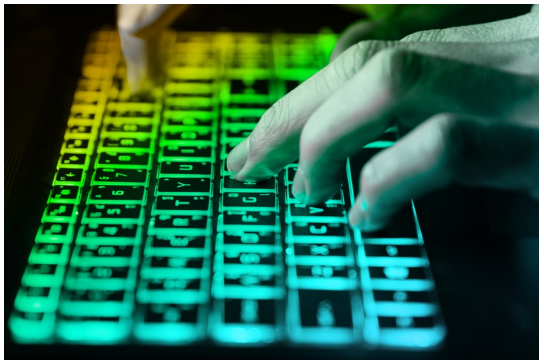
Other targets

Keyboards

USB communication

…



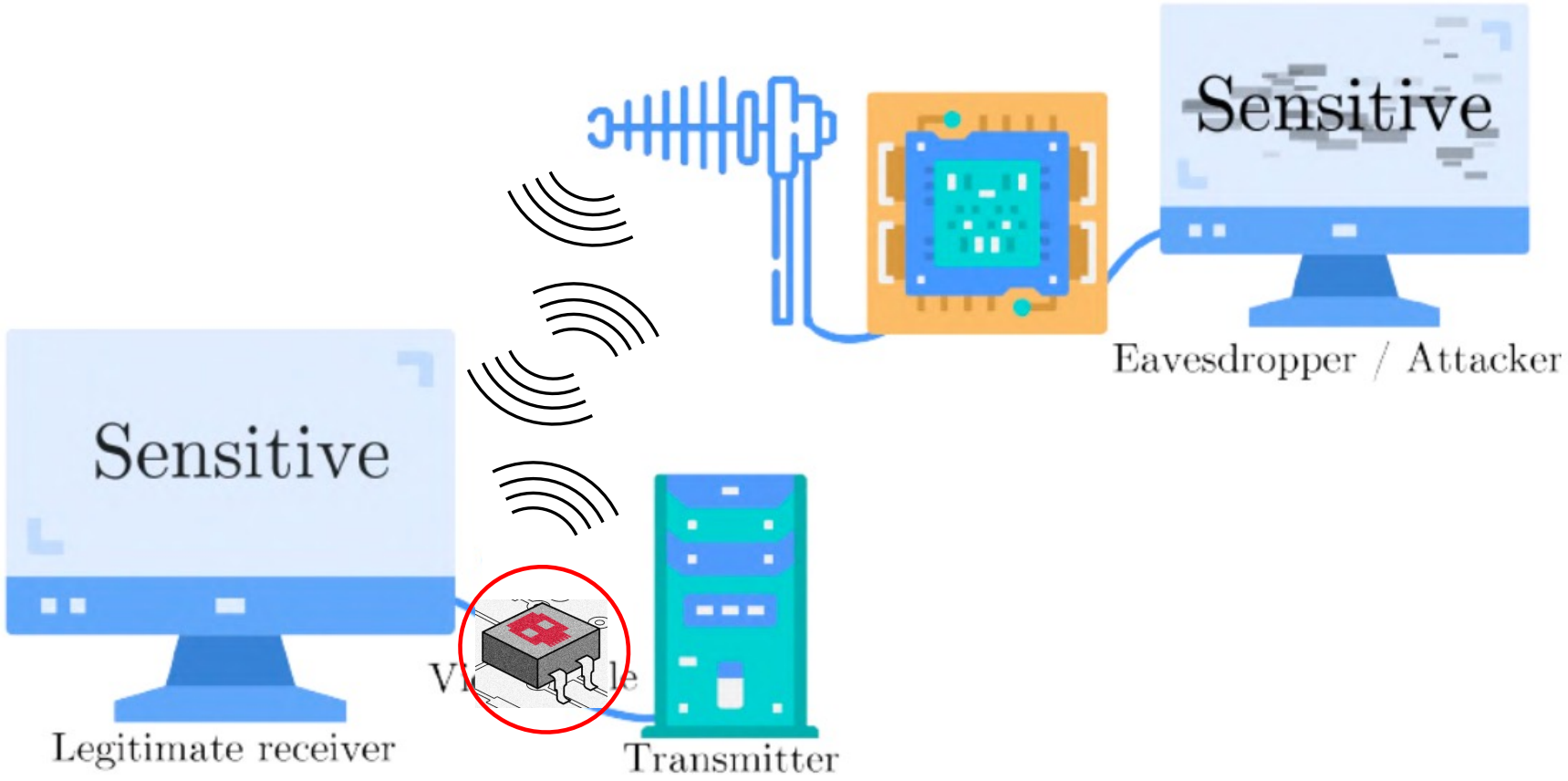


Limitations of TEMPEST attacks

The success depends on the target, its position, its coupling with the environment…

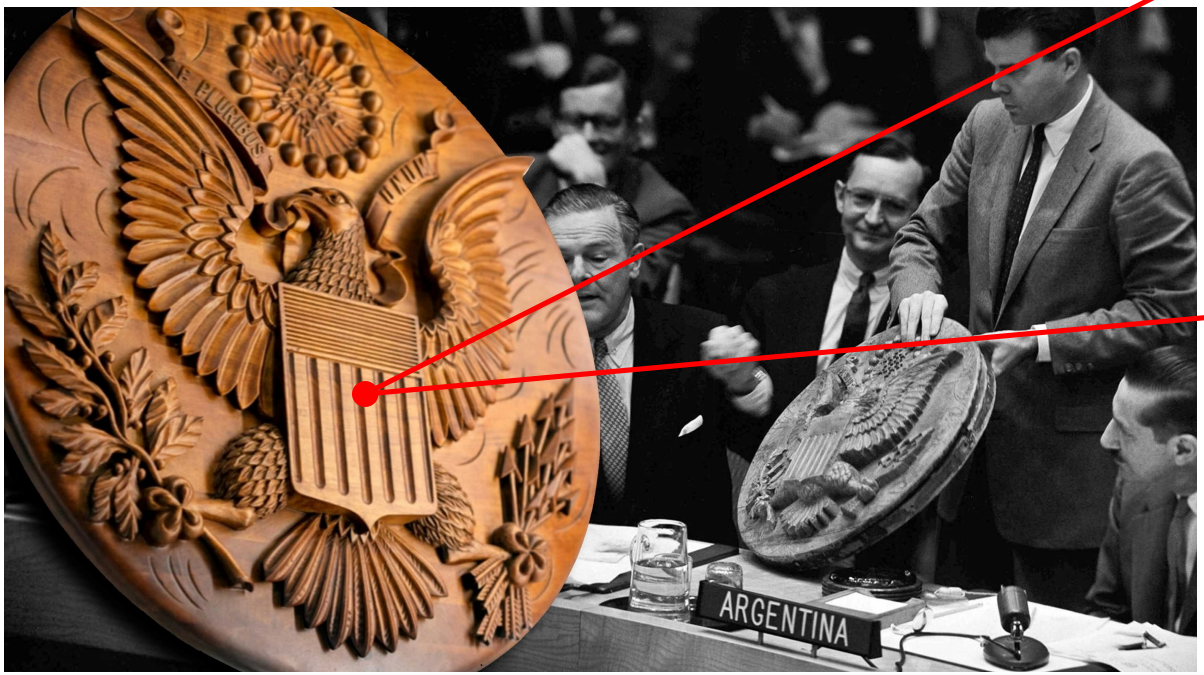
RF Retroreflector Attack (RFRA)

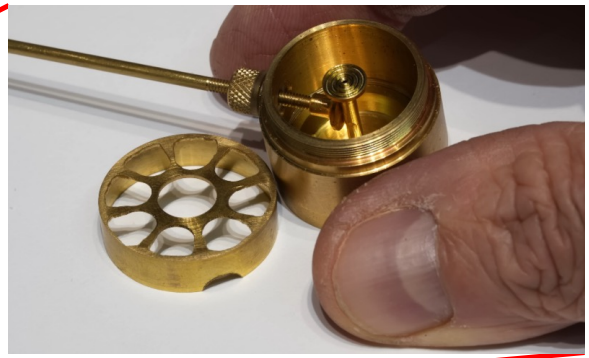
From TEMPEST… to RFRA



RF Retroreflector Attack (RFRA)

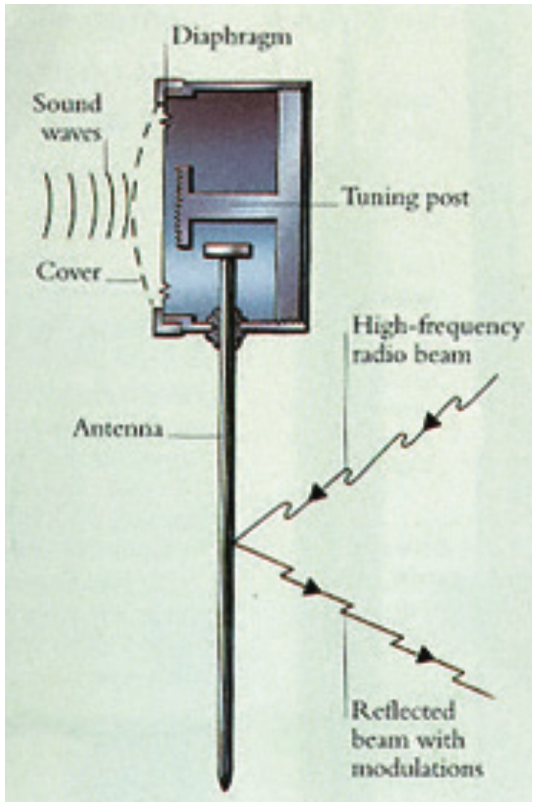
The Thing (1945-1952) aka The Great Seal Bug

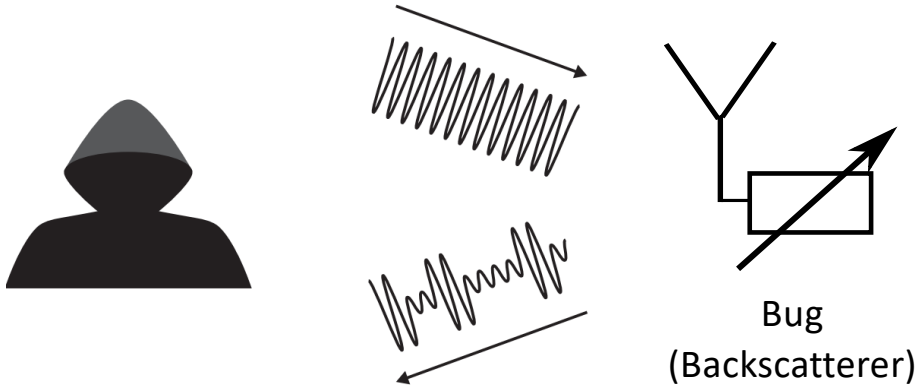




RF Retroreflector Attack (RFRA)

The Thing (1945-1952) aka The Great Seal Bug





- Purely passive
- Hard to detect

RF Retroreflector Attack (RFRA)

ANT Catalog

https://www.eff.org/document/20131230-appelbaum-nsa-ant-catalog

Classified NSA documents leaked in 2013 (in parallel of Edward Snowden)

SURLYSPAWN

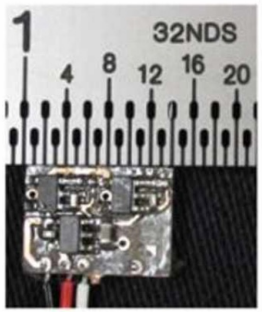
ANT Product Data

(TS//SI//REL TO USA,FVEY) Data RF retro-reflector. Provides return modulated with target data (keyboard, low data rate digital device) when illuminated with radar.

07 Apr 2009

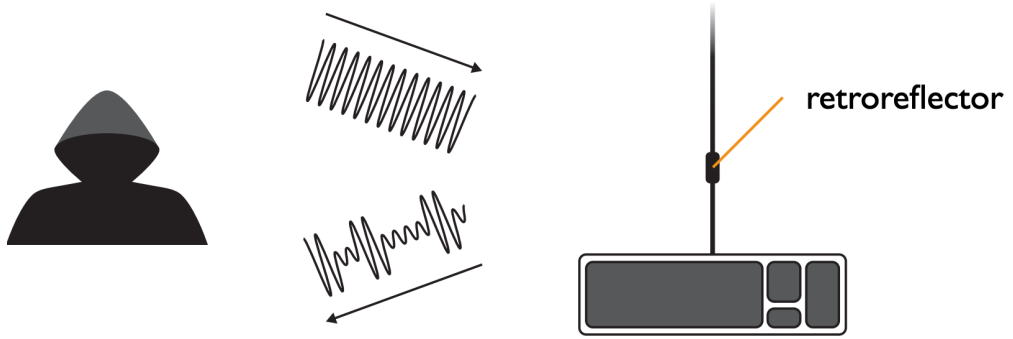
(U) Capabilities

(TS//SI//REL TO USA,FVEY) SURLYSPAWN has the capability to gather keystrokes without requiring any software running on the targeted system. It also only requires that the targeted system be touched once. The retro-reflector is compatible with both USB and PS/2 keyboards. The simplicity of the design allows the form factor to be tailored for specific operational requirements. Future capabilities will include laptop keyboards.



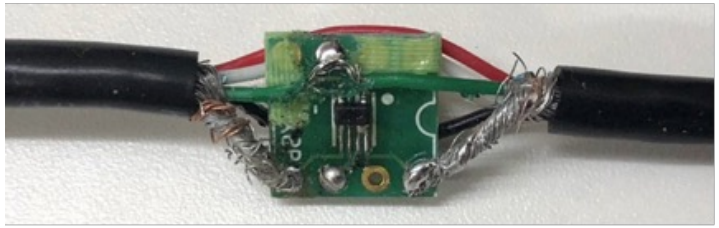
(U) Concept of Operation

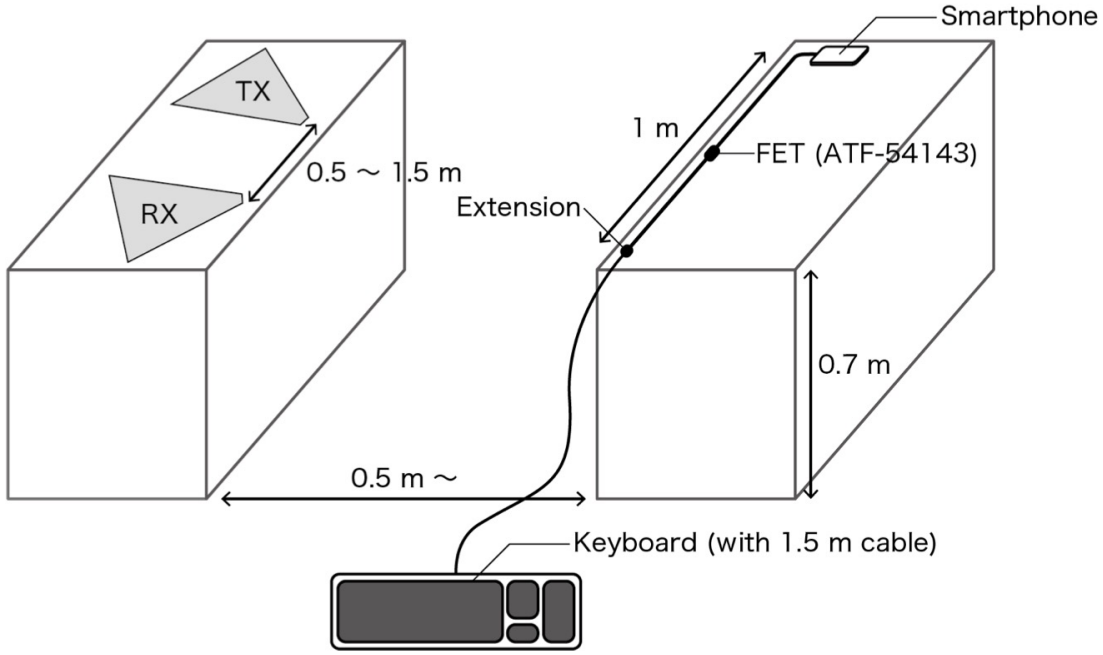
(TS//SI//REL TO USA,FVEY) The board taps into the data line from the keyboard to the processor. The board generates a square wave oscillating at a preset frequency. The data-line signal is used to shift the square wave frequency higher or lower, depending on the level of the data-line signal. The square wave, in essence, becomes frequency shift keyed (FSK). When the unit is illuminated by a CW signal from a nearby radar, the illuminating signal is amplitude-modulated (AM) with this square wave. The signal is re-radiated, where it is received by the radar, demodulated, and the demodulated signal is processed to recover the keystrokes. SURLYSPAWN is part of the ANGRYNEIGHBOR family of radar retro-reflectors.

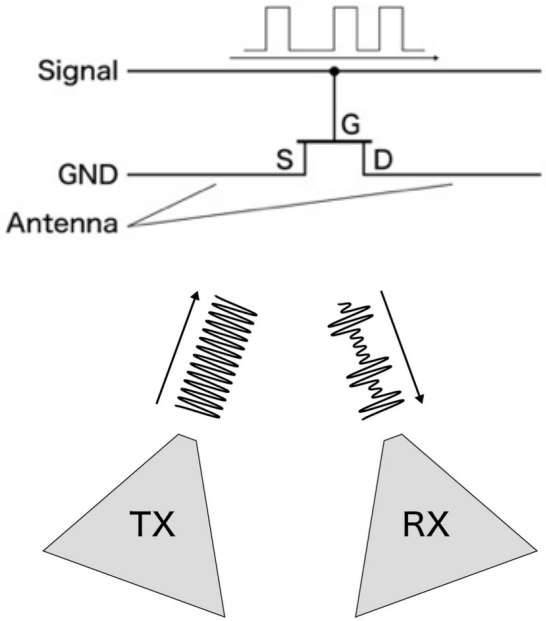


RF Retroreflector Attack (RFRA)

Academic work (2018)





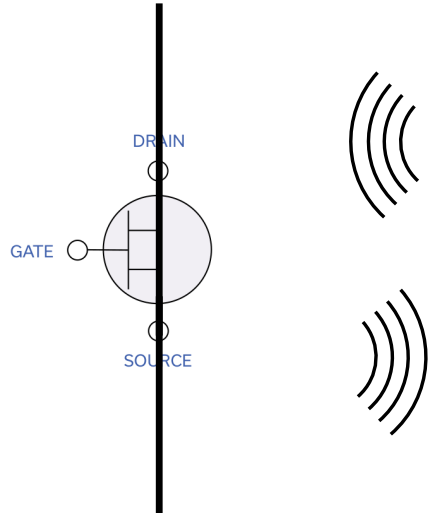


Satohiro Wakabayashi et al., "*A Feasibility Study of Radio-frequency Retroreflector Attack*", **USENIX WOOT**, 2018.

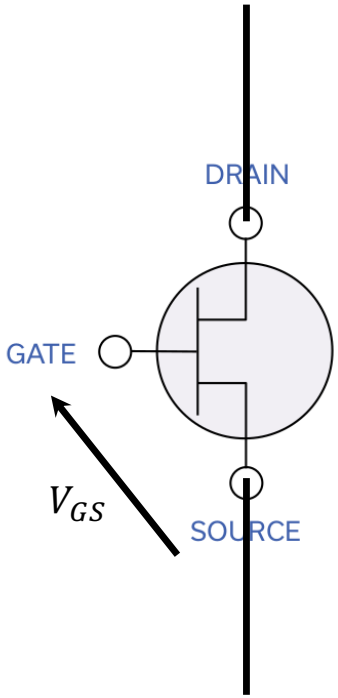
RF Retroreflector Attack (RFRA)

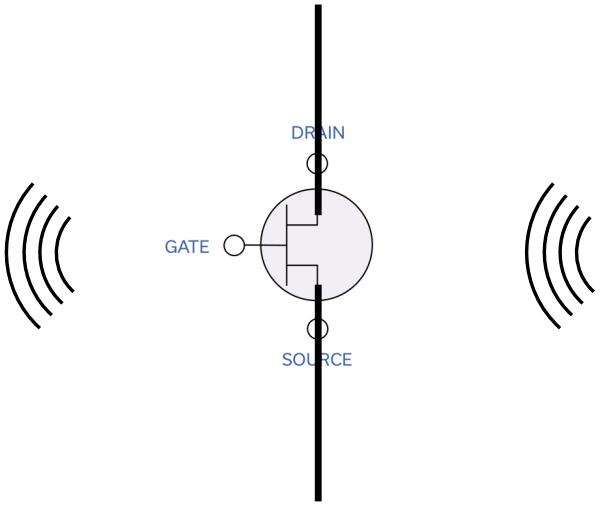
Basic explanation

$V_{GS} > 0.3$ V → Close



$V_{GS} < 0.3$ V → Open





Outline

I/. Introduction to EM Cybersecurity

A bit of history

TEMPEST attack on a VGA cable

Basic concept of a Radio-Frequency Retroreflector Attack (RFRA)

II/. RFRA

New trojan architecture

Multi trojans attacks

Retro Reflector Attacks

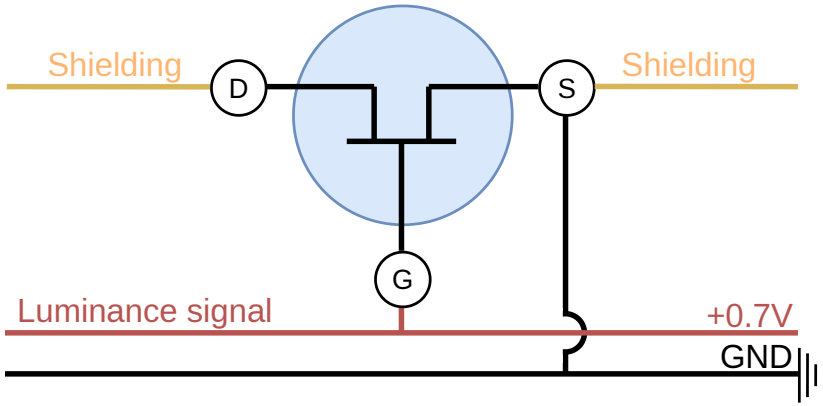
Remote data extraction through retroreflector hardware implants

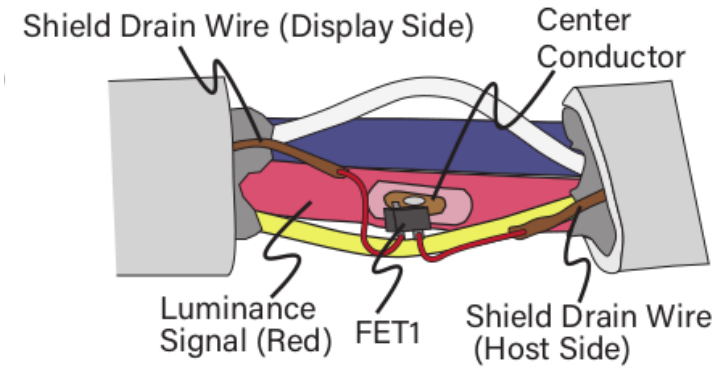
- SARRAZIN Francois :
francois.sarrazin@univ-rennes.fr

- GRANIER Pierre :
pierre.granier@univ-rennes.fr

FET Based

- V_{gs} bias applied by a data line
- Antenna made from the shielding connected to Drain and Source
- Dipole antenna with $+/-$ an impedance mismatch at its feed



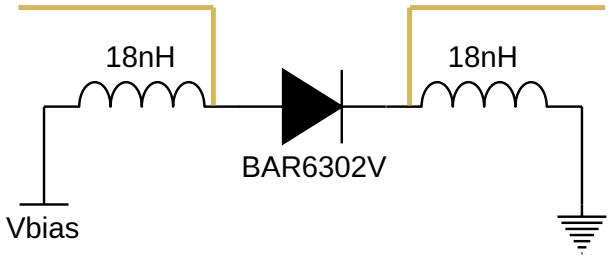


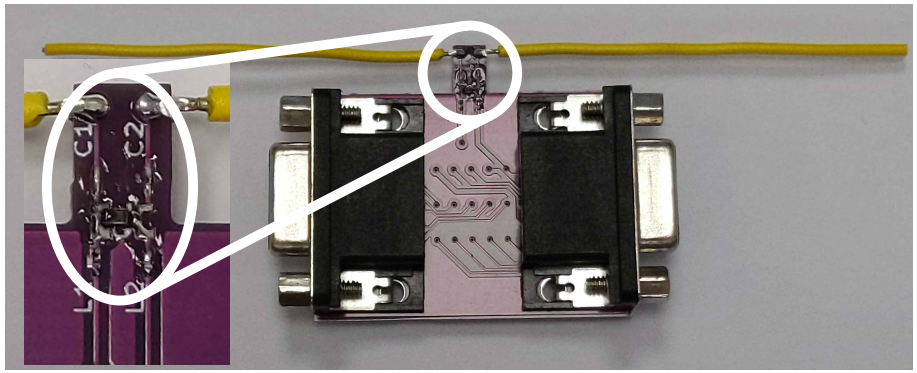
Credit: Yuichi Hayashi et al

Diode based Retroreflector

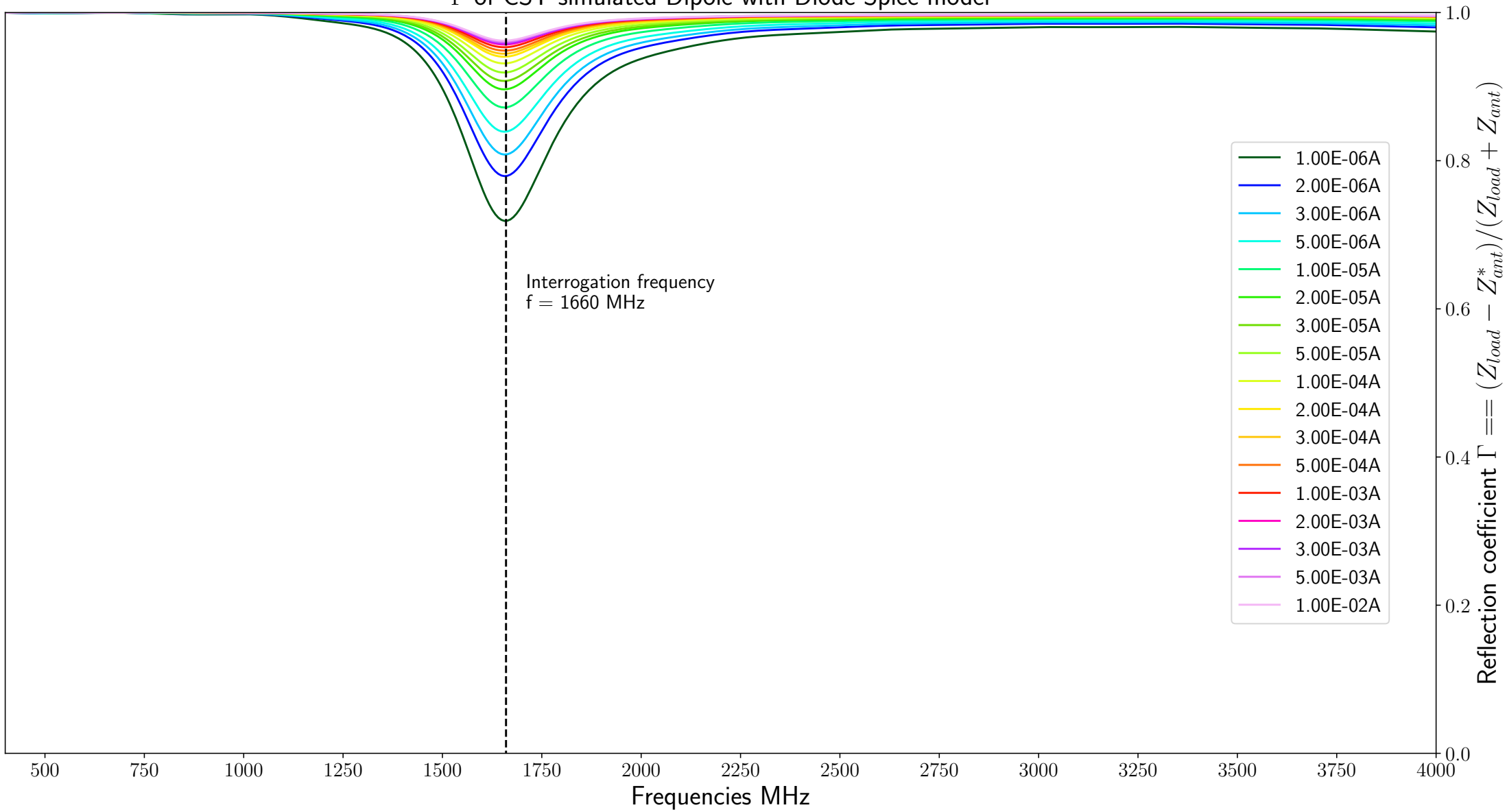
Retroreflector architecture and characterization

FET based implants with a V_{gs} and no V_{ds} bias are outside of the nominal behavior of a FET and is harder to characterize.
Switch to diode based Trojan.



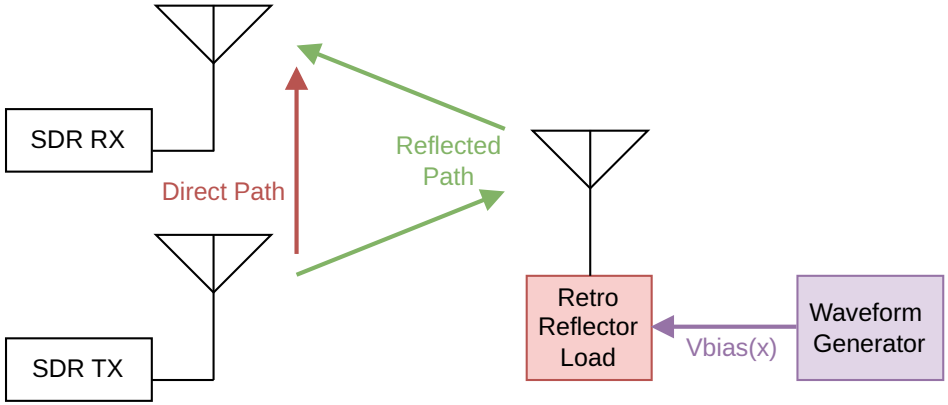


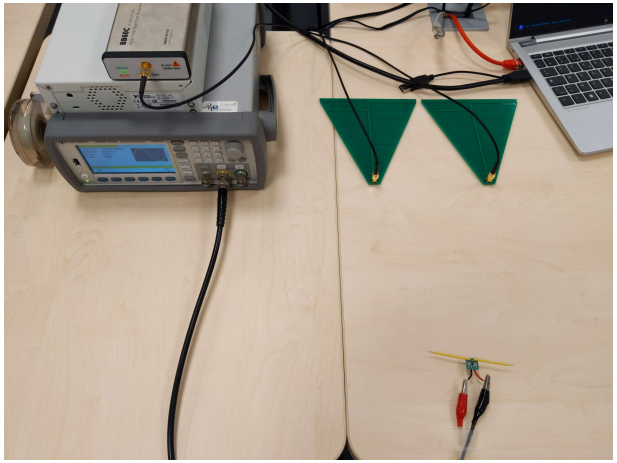
This change of architecture allows us to plan ahead using the Spice of our(s) component (BAR6302) and a simulation of our future antenna.


Γ of CST simulated Dipole with Diode Spice model
Interrogation frequency
f = 1660 MHz
1.00E-06A
2.00E-06A
3.00E-06A
5.00E-06A
1.00E-05A
2.00E-05A
3.00E-05A
5.00E-05A
1.00E-04A
2.00E-04A
3.00E-04A
5.00E-04A
1.00E-03A
2.00E-03A
3.00E-03A
5.00E-03A
1.00E-02A
500
750
1000
1250
1500
1750
2000
2250
2500
2750
3000
3250
3500
3750
4000
Frequencies MHz
0.0
0.2
0.4
0.6
0.8
1.0
Reflection coefficient Γ == $(Z_{load} - Z^*_{ant})/(Z_{load} + Z_{ant})$

Retroreflector Architecture and characterization

Retro Reflector usability across the RF spectrum is hard to measure with SDR because of the direct path between TX and RX.

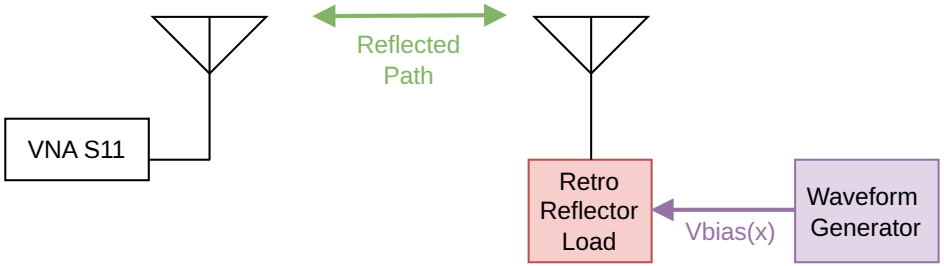




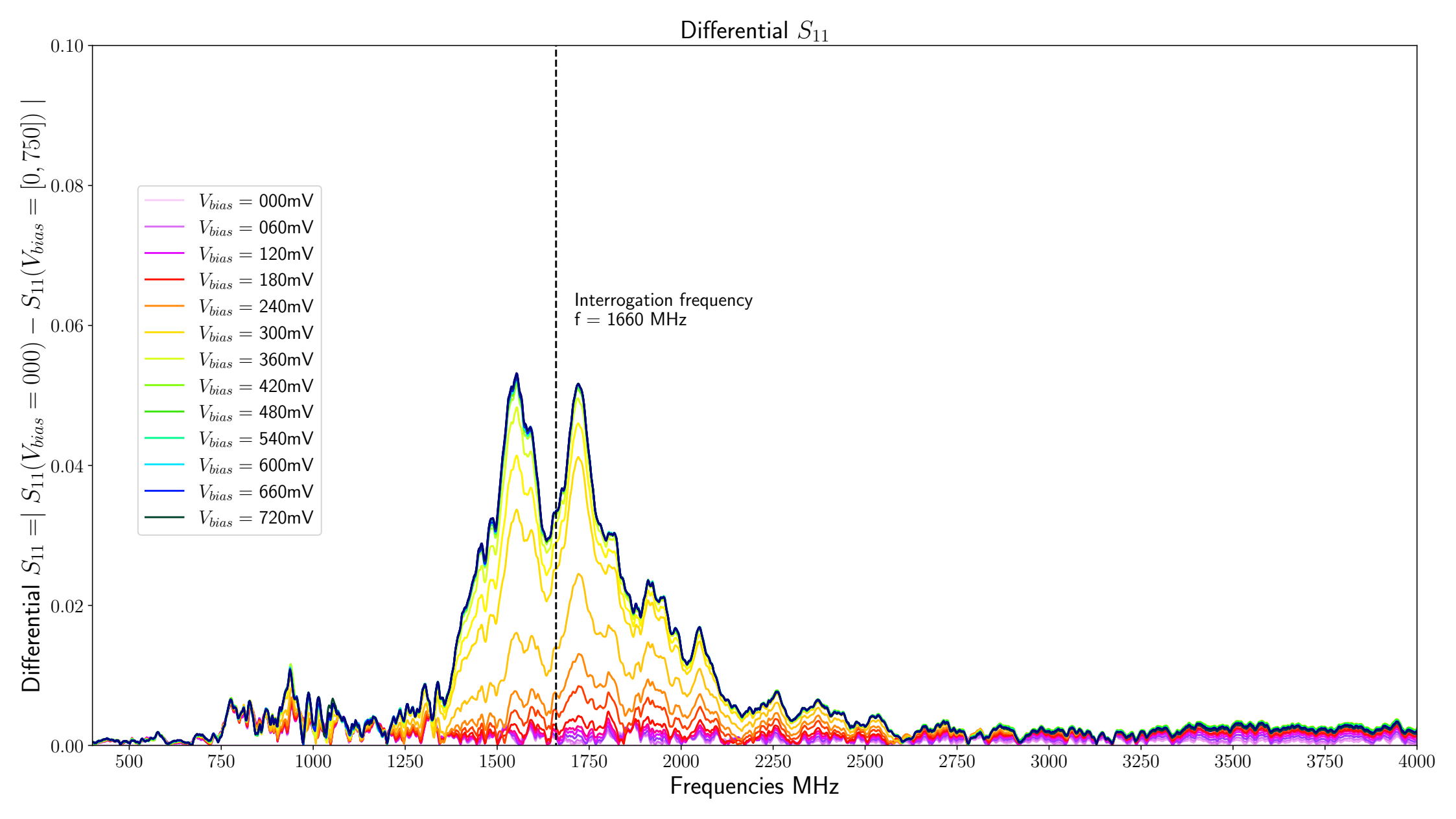
Instead, we rely on a VNA that can both send a pulse and monitor its reflection on the same channel.

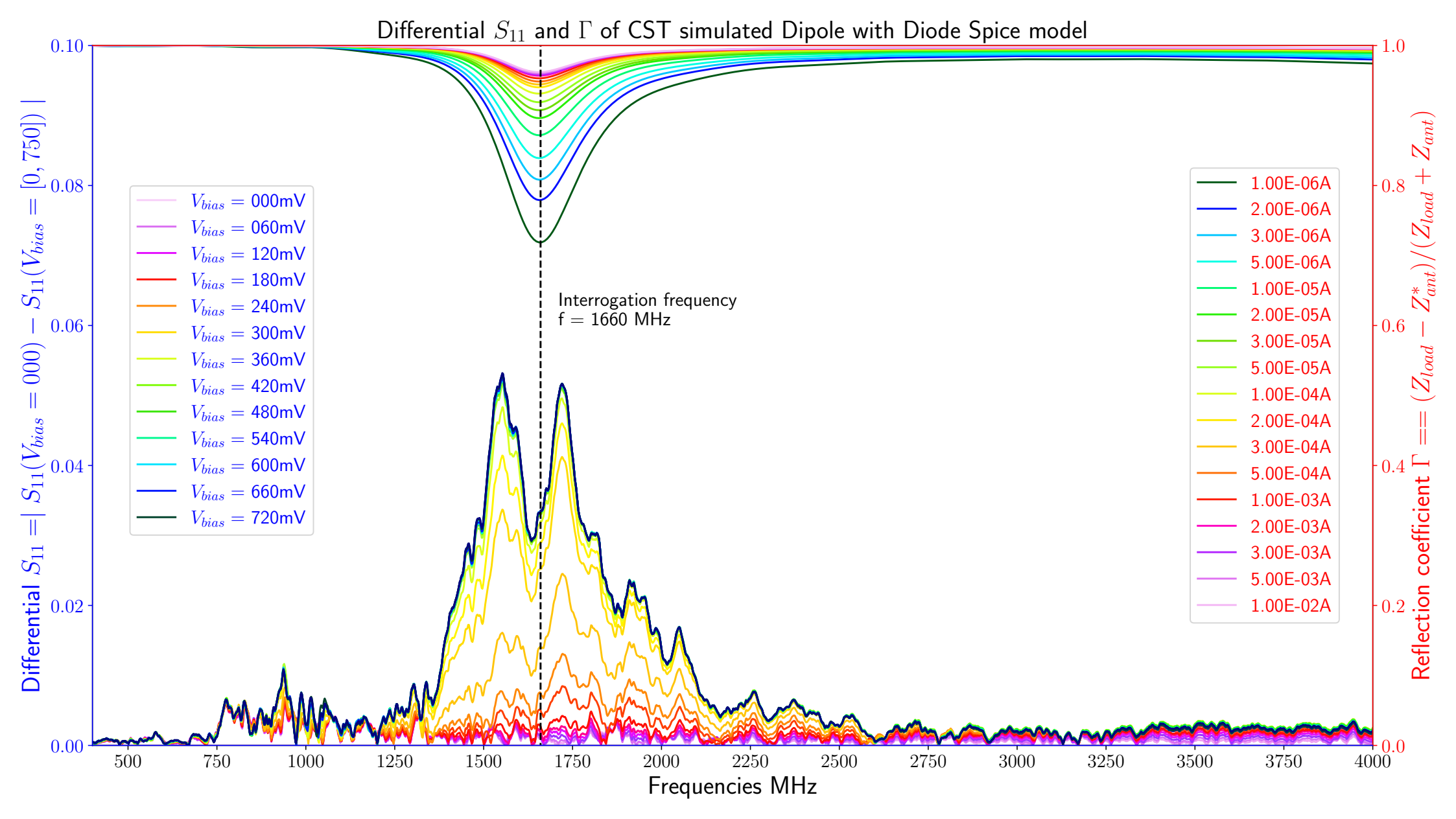
Retroreflector Architecture and characterization

This allows us to get its S_{11} for different V_{bias}.



(The VNA side antenna properties create some of the irregularities observed.)

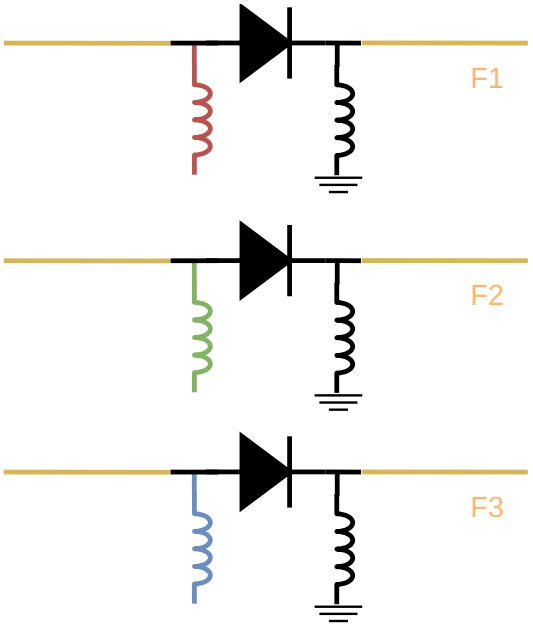

Differential S_{11}
Differential S_{11} =| $S_{11}(V_{bias} = 000) - S_{11}(V_{bias} = [0, 750])$ |
Frequencies MHz
Interrogation frequency
f = 1660 MHz
V_{bias} = 000mV
V_{bias} = 060mV
V_{bias} = 120mV
V_{bias} = 180mV
V_{bias} = 240mV
V_{bias} = 300mV
V_{bias} = 360mV
V_{bias} = 420mV
V_{bias} = 480mV
V_{bias} = 540mV
V_{bias} = 600mV
V_{bias} = 660mV
V_{bias} = 720mV
0.00
0.02
0.04
0.06
0.08
0.10
500
750
1000
1250
1500
1750
2000
2250
2500
2750
3000
3250
3500
3750
4000

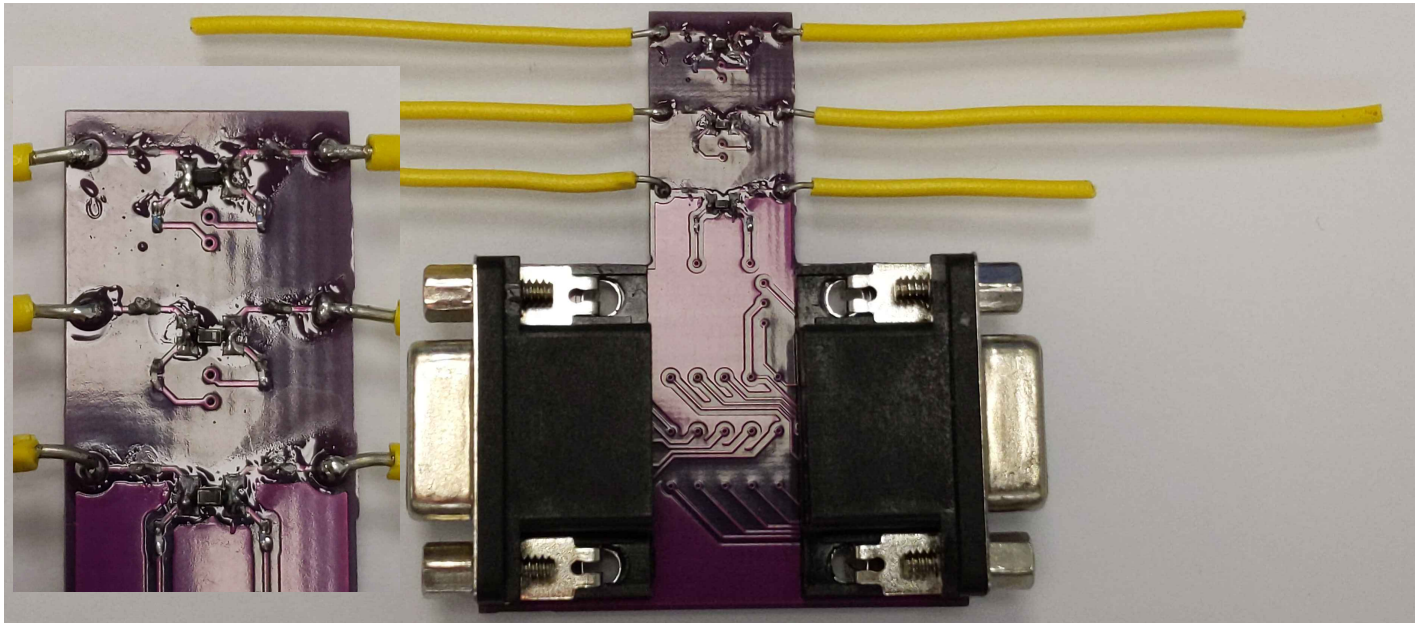

Differential S_{11} and Γ of CST simulated Dipole with Diode Spice model
Differential S_{11} =| $S_{11}(V_{bias} = 000) - S_{11}(V_{bias} = [0, 750])$ |
Reflection coefficient $\Gamma == (Z_{load} - Z^*_{ant})/(Z_{load} + Z_{ant})$
Frequencies MHz
Interrogation frequency
f = 1660 MHz
V_{bias} = 000mV
V_{bias} = 060mV
V_{bias} = 120mV
V_{bias} = 180mV
V_{bias} = 240mV
V_{bias} = 300mV
V_{bias} = 360mV
V_{bias} = 420mV
V_{bias} = 480mV
V_{bias} = 540mV
V_{bias} = 600mV
V_{bias} = 660mV
V_{bias} = 720mV
1.00E-06A
2.00E-06A
3.00E-06A
5.00E-06A
1.00E-05A
2.00E-05A
3.00E-05A
5.00E-05A
1.00E-04A
2.00E-04A
3.00E-04A
5.00E-04A
1.00E-03A
2.00E-03A
3.00E-03A
5.00E-03A
1.00E-02A
0.10
0.08
0.06
0.04
0.02
0.00
1.0
0.8
0.6
0.4
0.2
0.0
500
750
1000
1250
1500
1750
2000
2250
2500
2750
3000
3250
3500
3750
4000

Multi trojans

RFRA RGB (Multi Trojan)

Now that we can plan multiple implants at different frequencies, we can interrogate different data line (same target or not).

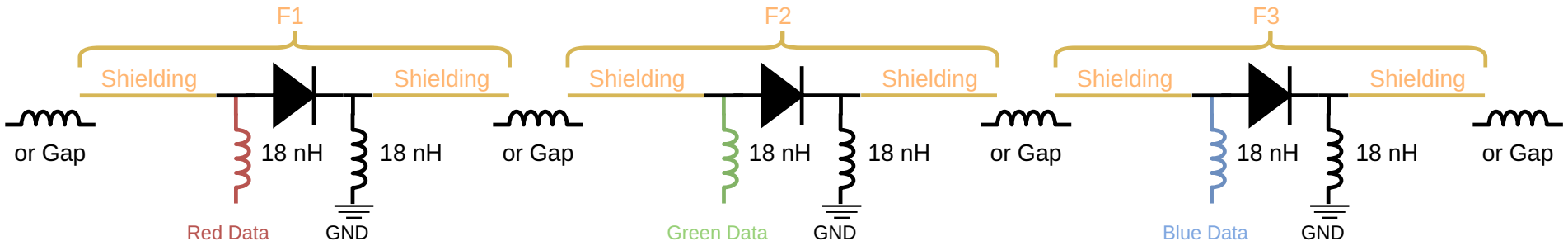


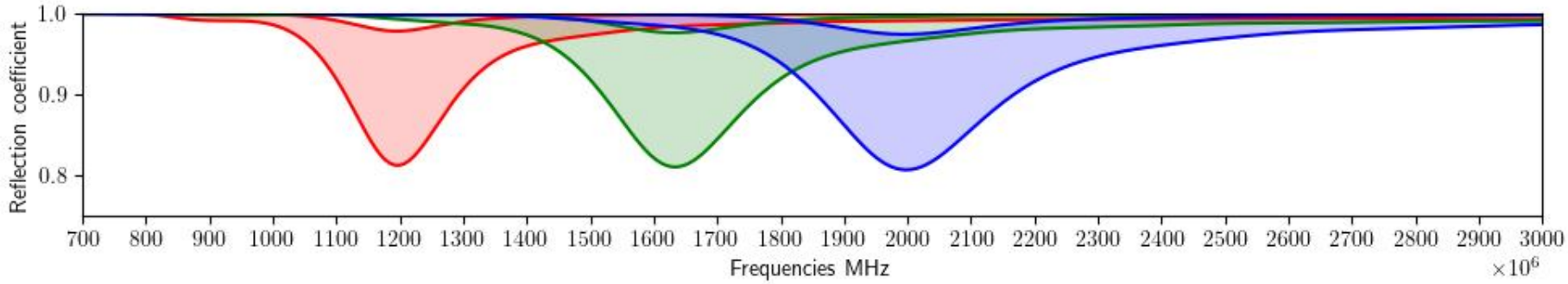


RFRA RGB (Multi Trojan)

With a diode-based architecture, we were able to have a proof of concept for collocated triple Trojan.

This make Trojan on different data lines of one or multiple targets possible.

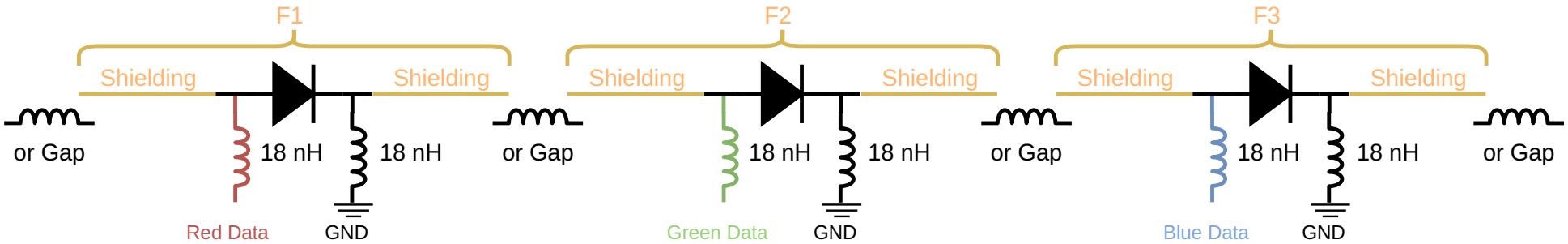


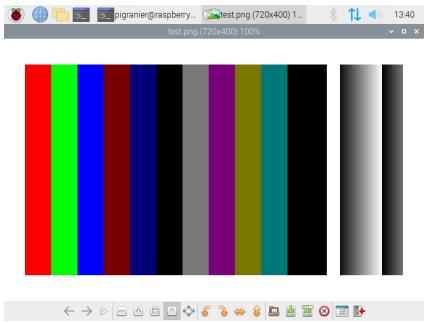


RFRA RGB (Multi Trojan)

With a diode-based architecture, we were able to have a proof of concept for collocated triple Trojan.

This make Trojan on different data lines of one or multiple targets possible.





Get N Frame at F1

Get N Frame at F2

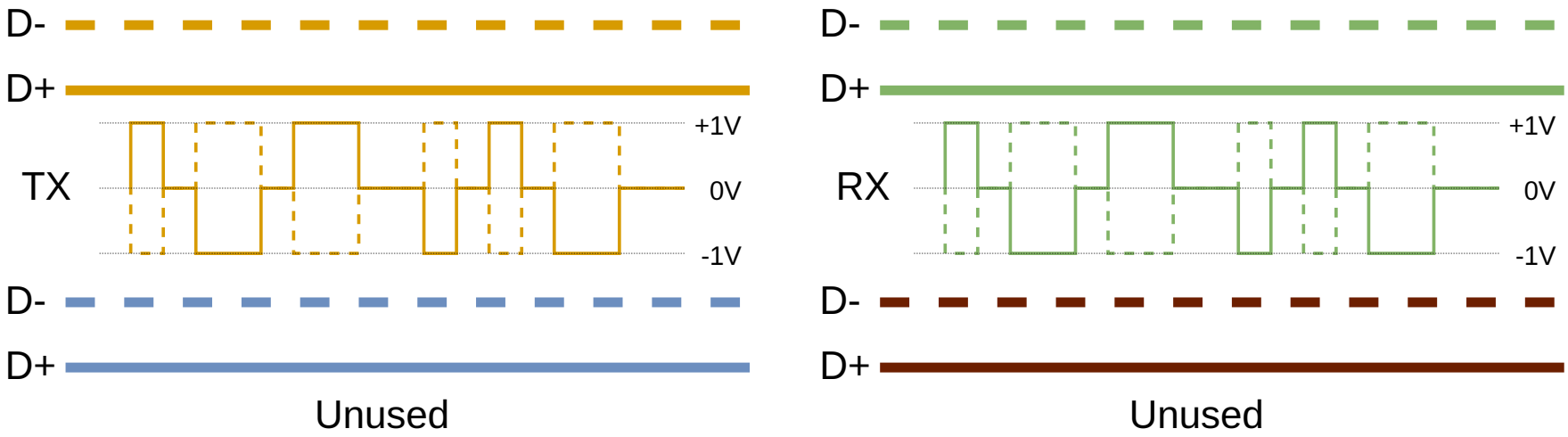
Get N Frame at F3

RFRA

Fast Ethernet

Ethernet 100 Base-TX Trojan

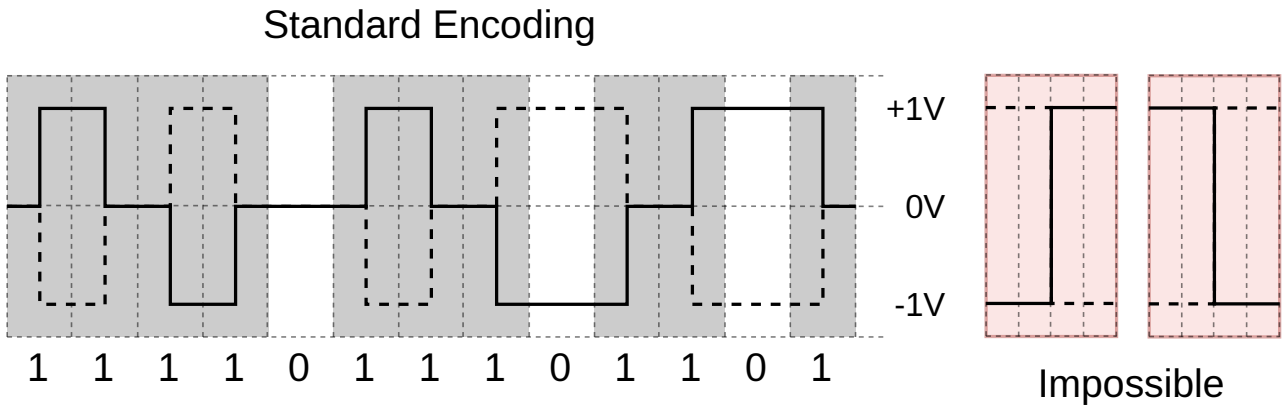
125 Mega symbol per second (100 Mbit/s) over two differential pairs (TX and RX).



Two unused pairs (will be recycled to host the antenna part in future work).

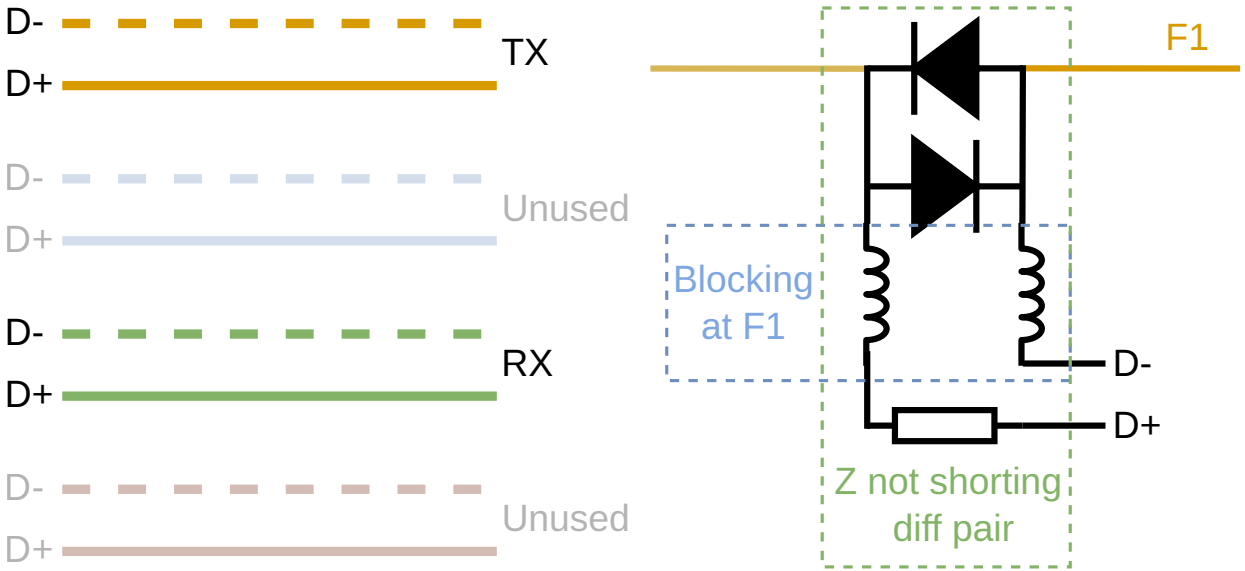
100 Base-Tx logic encoding only check if a logic-level transition occurs.

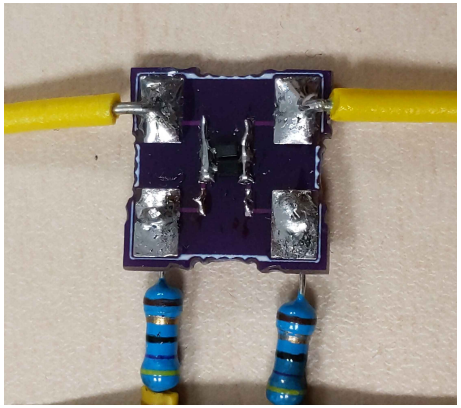
Transition $\rightarrow$ 1 ; No transition $\rightarrow$ 0



After $D^+ \neq D^-$ a transition will always go to $D^+ = D^-$.

If $D^+ \neq D^-$ next transition will go to $D^+ = D^-$.
We only need to discriminate $D^+ \neq D^-$ from $D^+ = D^-$.

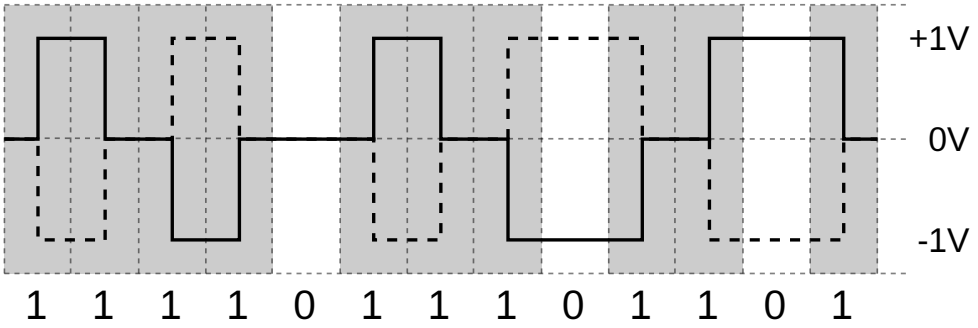




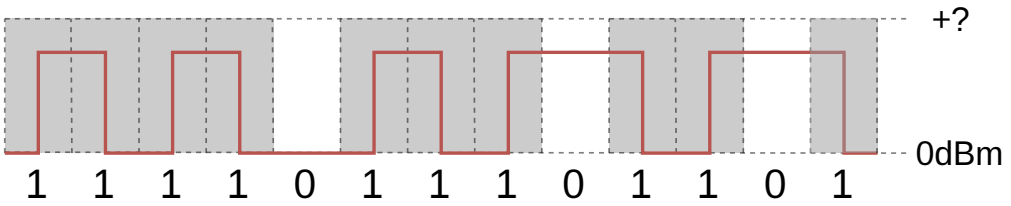
Fast Ethernet Decoding

If $D^+ \neq D^-$ next transition will go to $D^+ = D^-$.
We only need to discriminate $D^+ \neq D^-$ from $D^+ = D^-$.

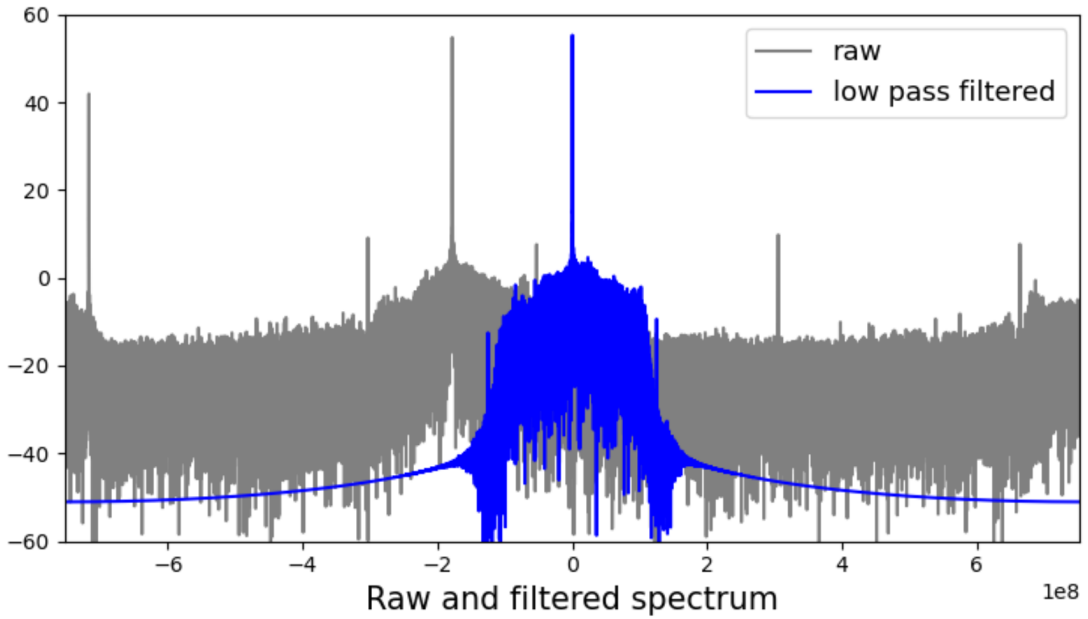
Standard Encoding



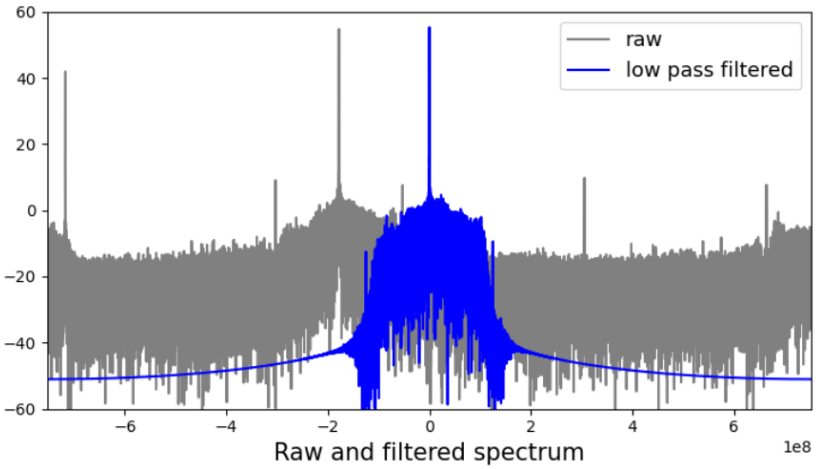
Retro Reflected states

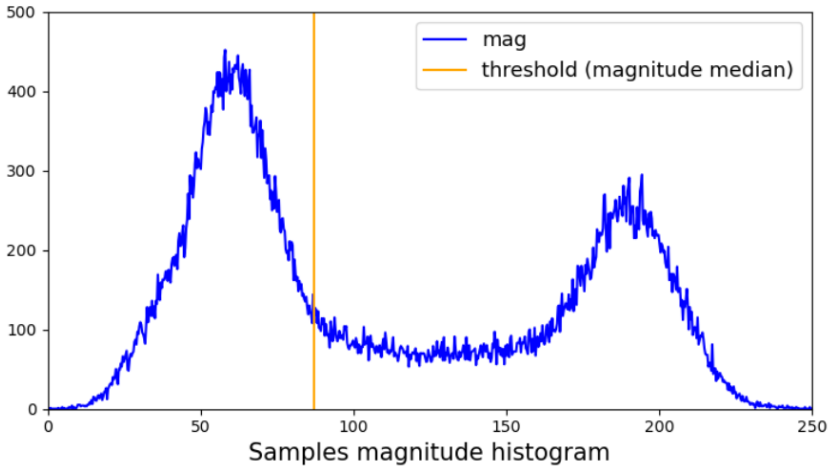


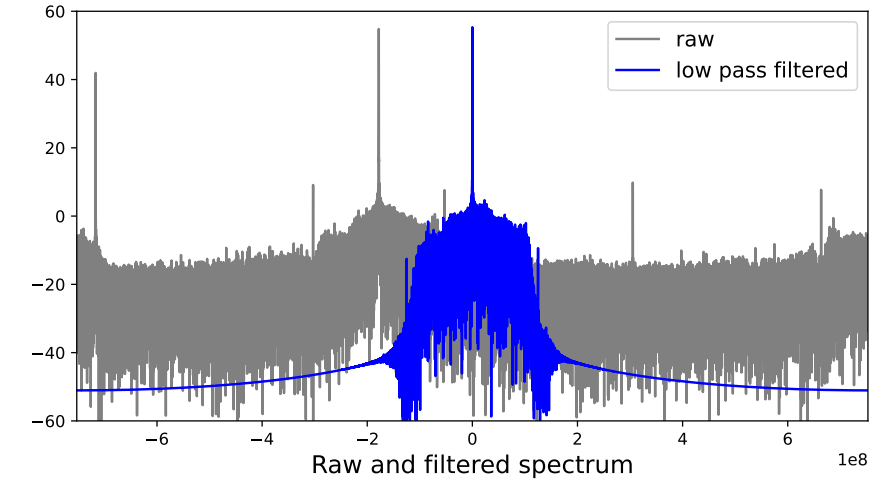
Over-sampling is almost mandatory here, we sample at 1.25Gsp.
This implies filtering all but the 250 MHz of useful frequencies.

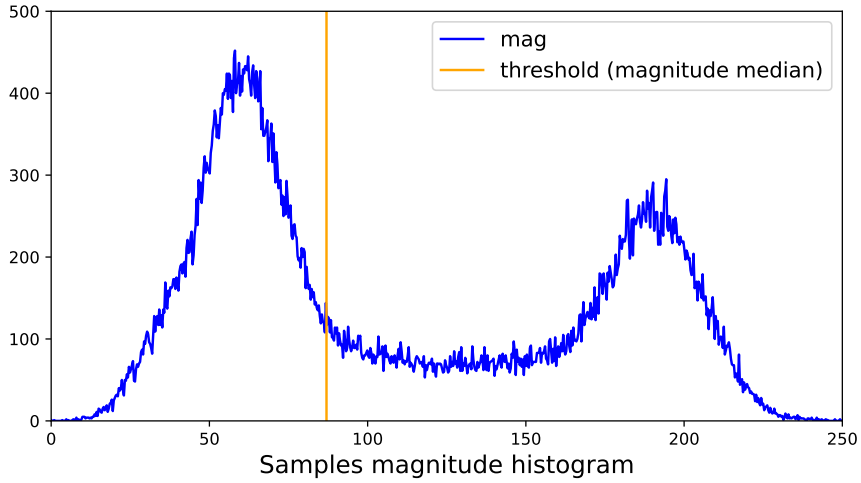


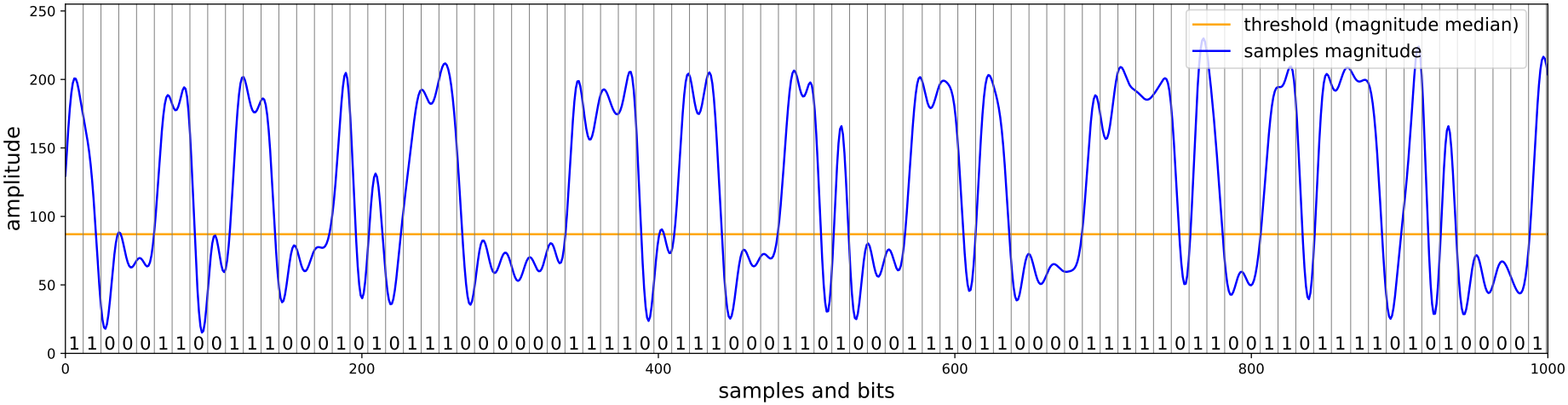
The median of samples magnitude will be our threshold for affecting bit values.






raw
low pass filtered
Raw and filtered spectrum
1e8

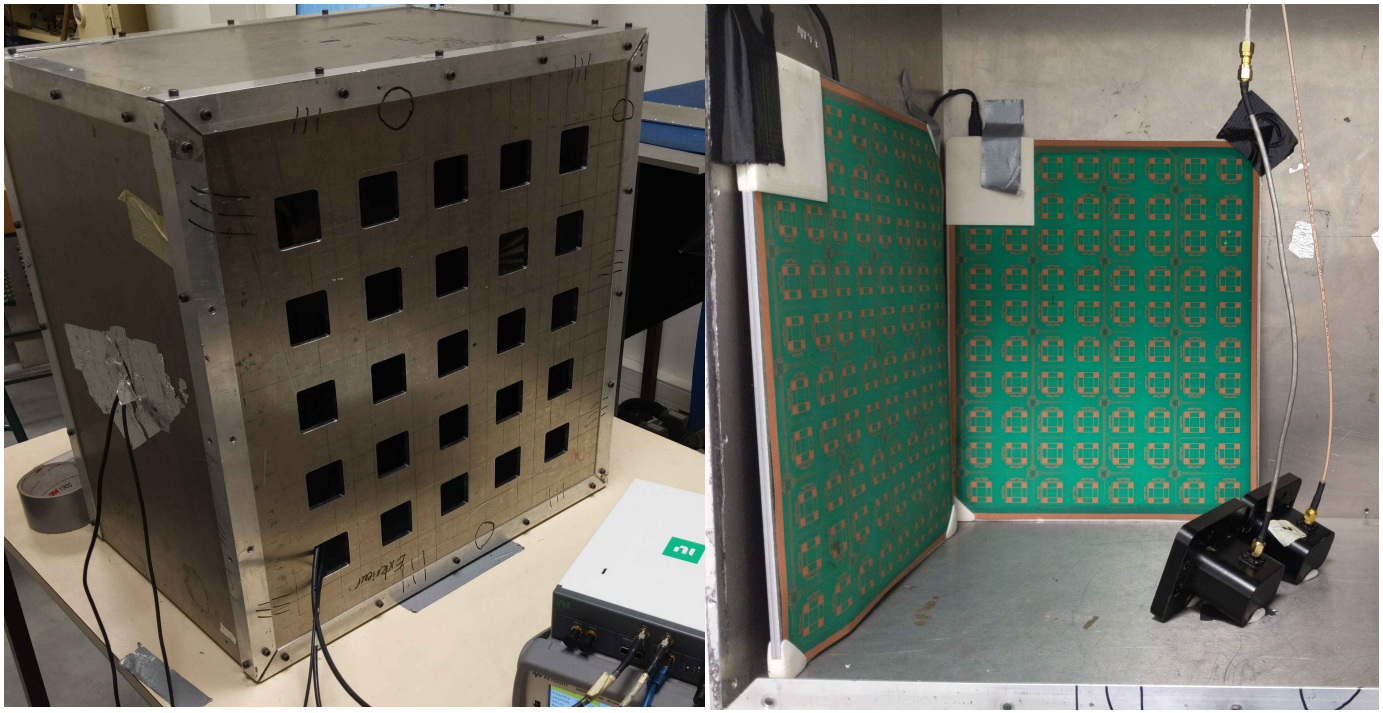

mag
threshold (magnitude median)
Samples magnitude histogram


threshold (magnitude median)
samples magnitude
amplitude
samples and bits
1 1 0 0 0 1 1 0 0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 0 0 0 0 1 1 1 1 0 0 1 1 1 0 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0 0 1 1 1 1 1 0 1 1 0 0 1 1 0 1 1 1 1 0 1 0 1 0 0 0 0 1

Focalization through a scattering medium

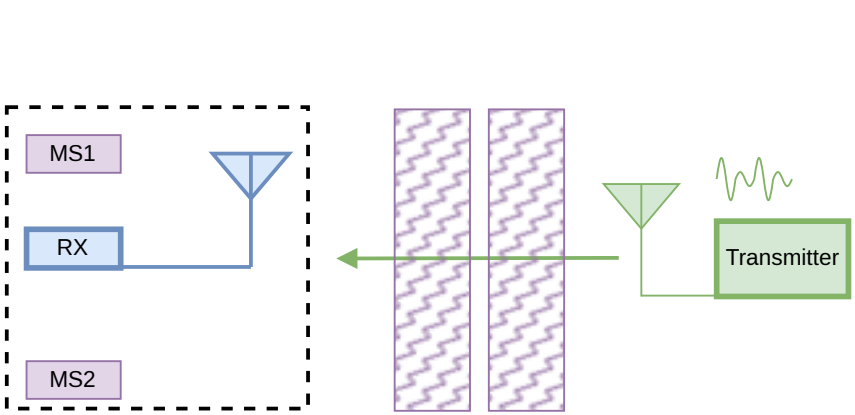
Focalization through scattering medium

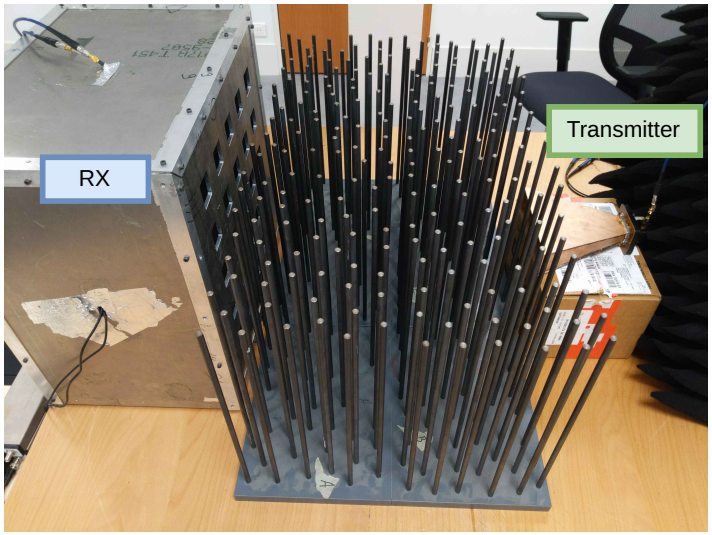
How to shape a wavefront through a complex environment toward a Trojan or leakage source ?



Focalization through scattering medium

Wavefront shaping to eavesdrop a transmitter behind a scattering medium.

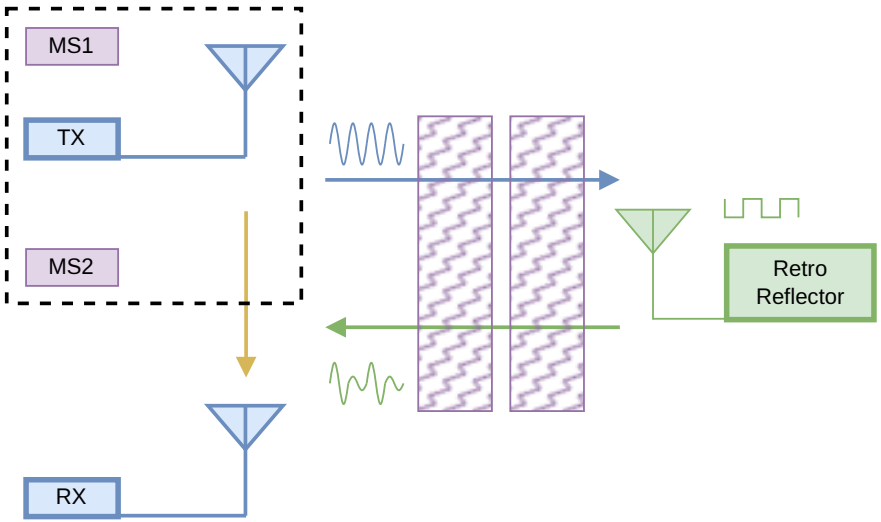


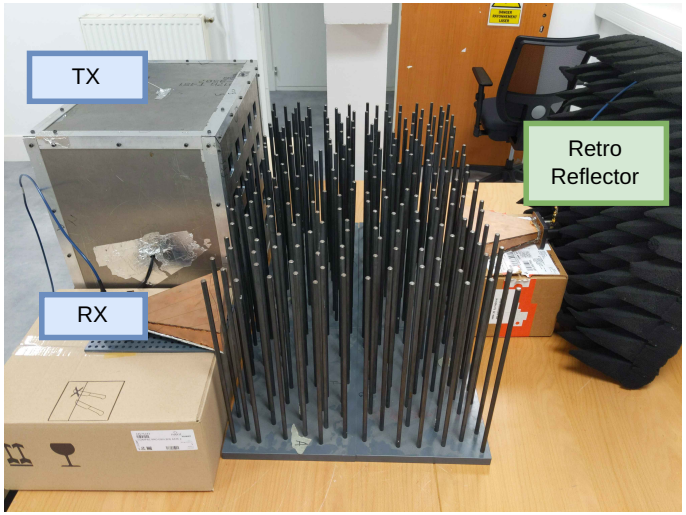


Post optimization we get around a 10 dB gain compared to a simple horn antenna.

Focalization through scattering medium

Wavefront shaping to interrogate a backscattering element behind a scattering medium.

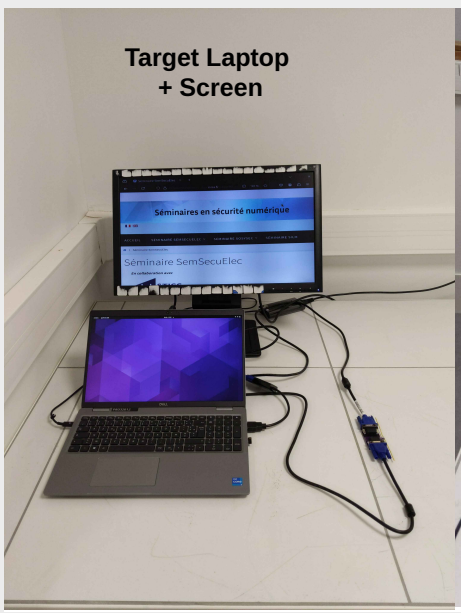


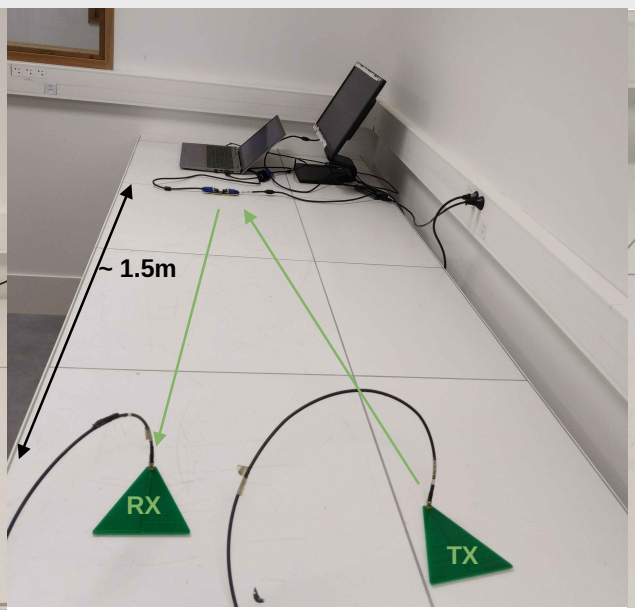


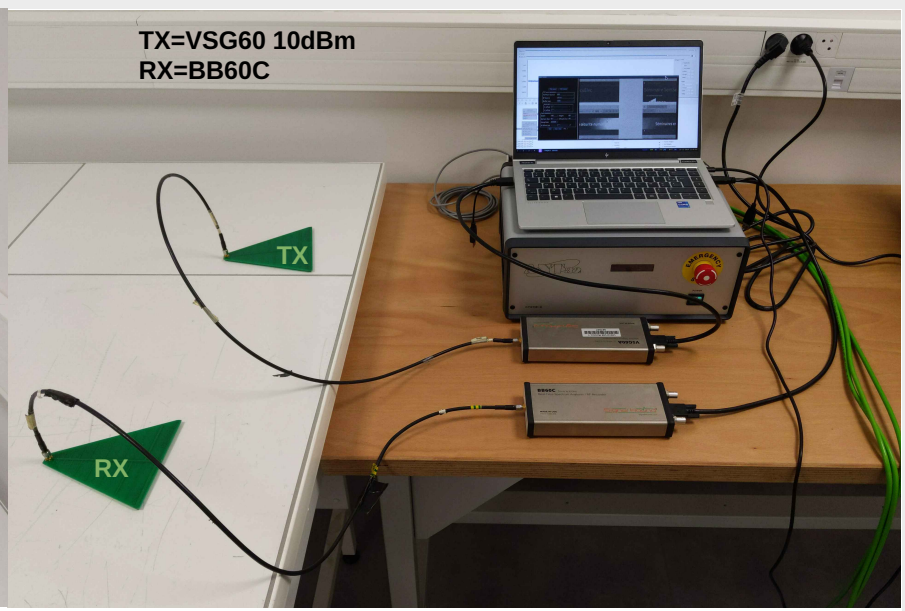
Harder due to the direct path between TX and RX.

RFRA Monochrome demo

RFRA Monochrome ~~demo~~ video







Retro Reflector Attacks

Remote data extraction through retroreflector hardware implants

- SARRAZIN Francois :
francois.sarrazin@univ-rennes.fr

- GRANIER Pierre :
pierre.granier@univ-rennes.fr