Ridiculous Radios

Dominic Spill (@dominicgs)

Thanks

Mike Walters

Ang Cui

Schuyler St. Leger

Matt Ettus

Jared Boone

Root Killah

Sergey Bratus

Travis Goodspeed

Taylor Streetman

Jacob Graves

Piotr Esden-Tempski

Michael Ossmann

Who am I?

Dominic Spill

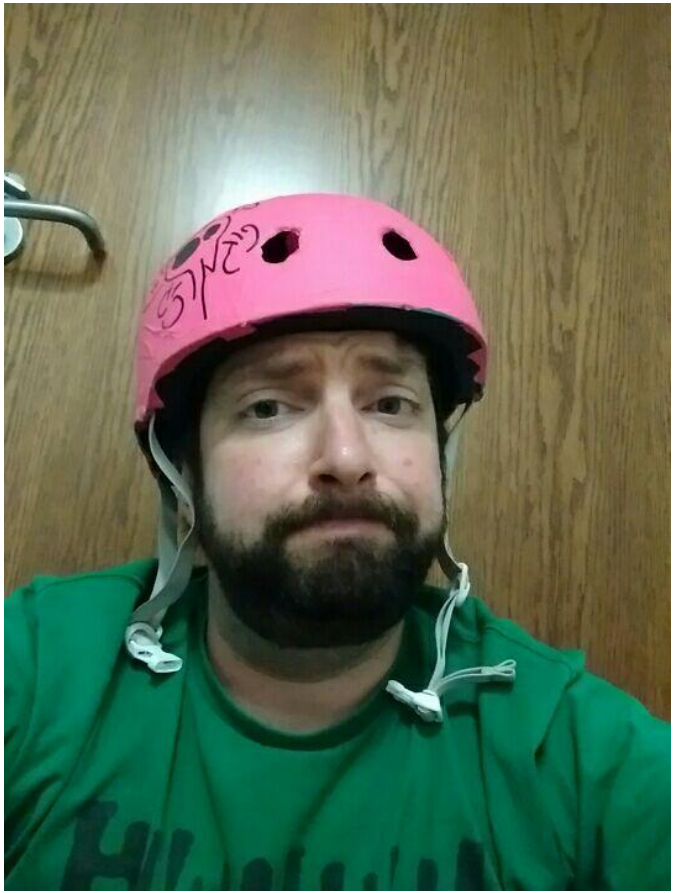
Security Researcher at Great Scott Gadgets

Investigating communication protocols - IR, RF, wired networks

Firmware and software for HackRF, Ubertooth, GreatFET

fcc.io

EMF Camp



Ridiculous things in this presentation

Revolting Receivers:

- Breadboard SDR
- 1-bit SDR

Terrible Transmitters:

- Clock Signal FSK
- Delay Line PSK

Disclaimer

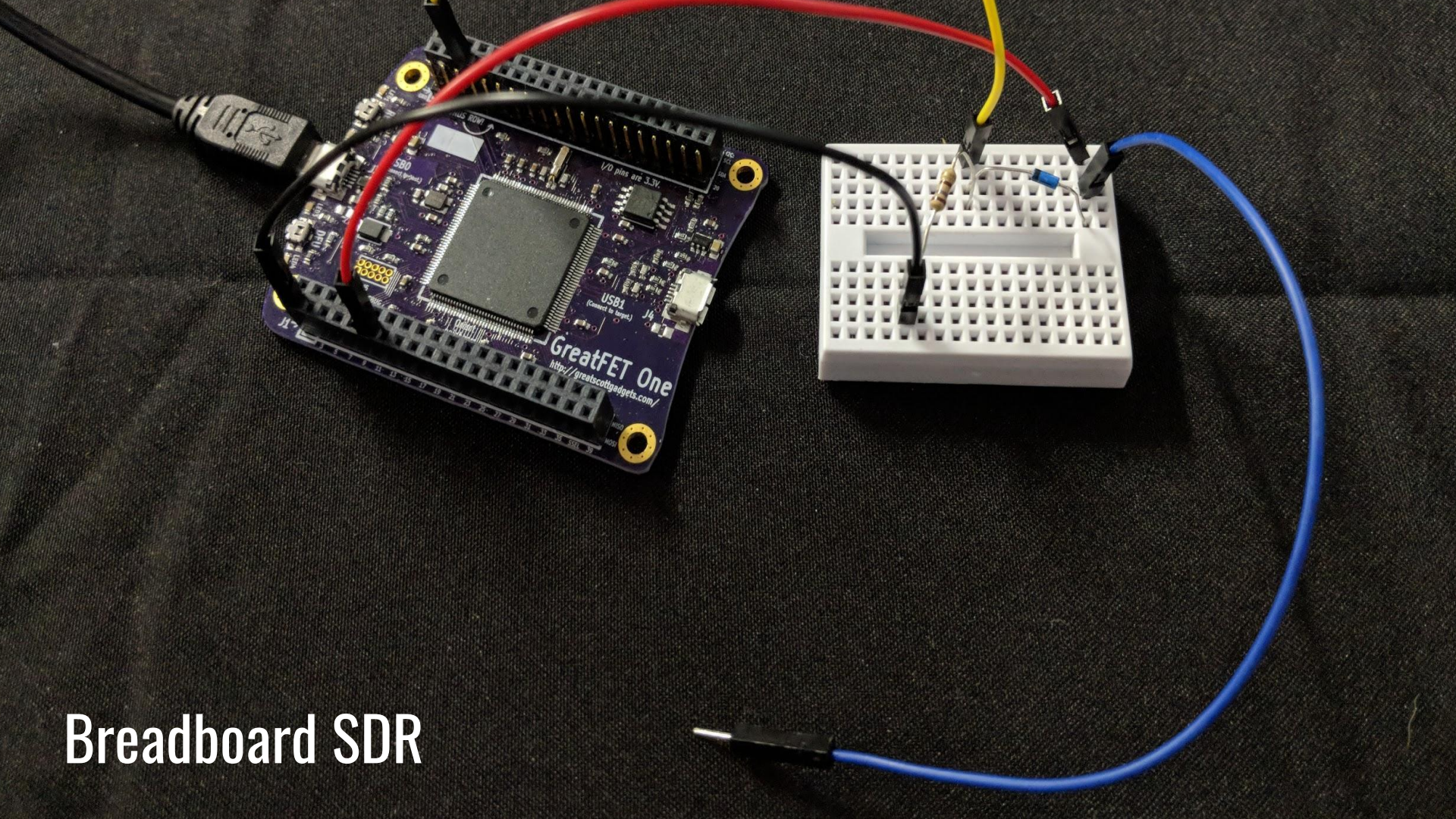
Know (and obey) your local laws

Scenario

Cheap microcontrollers are everywhere, they have Analog to Digital Converters (ADC) and speak USB.

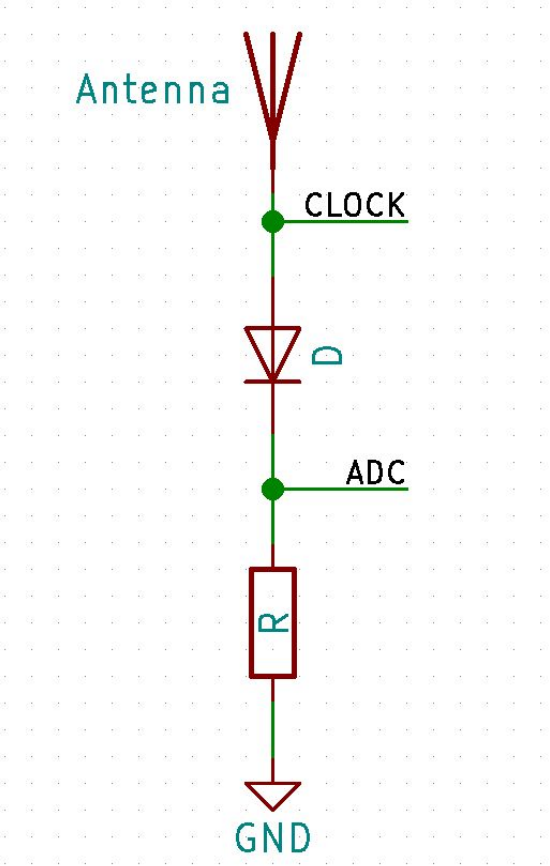
Can we build a radio receiver out of these microcontrollers?

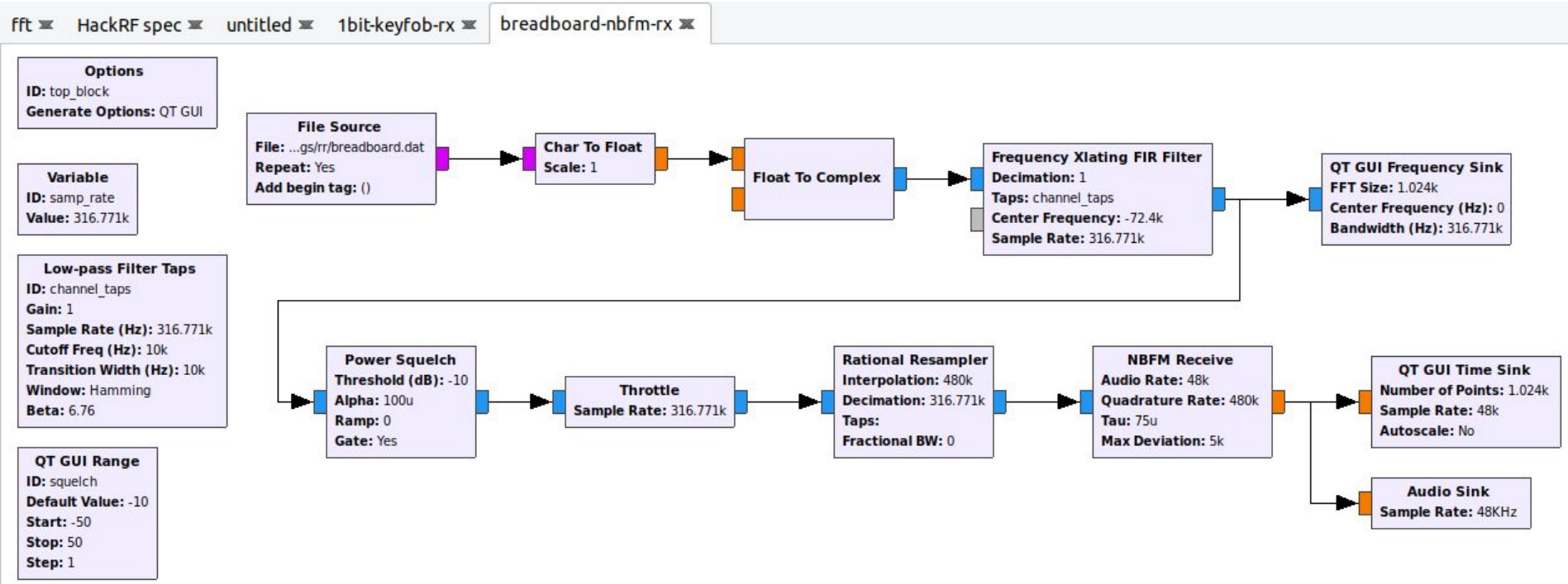
Breadboard SDR



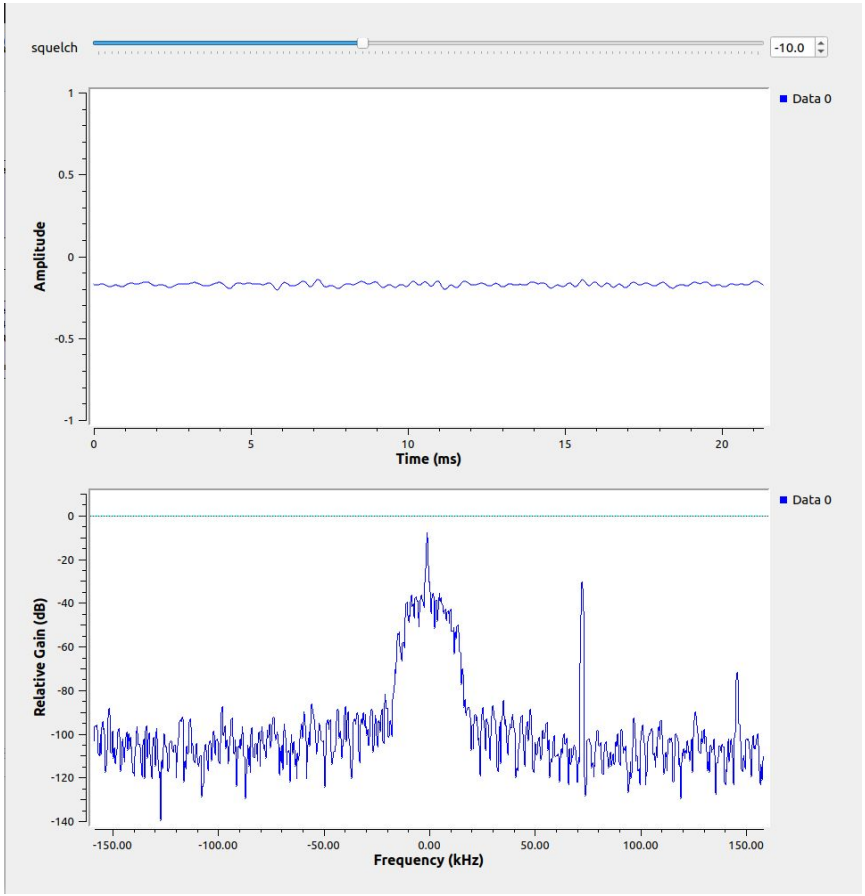
Breadboard SDR

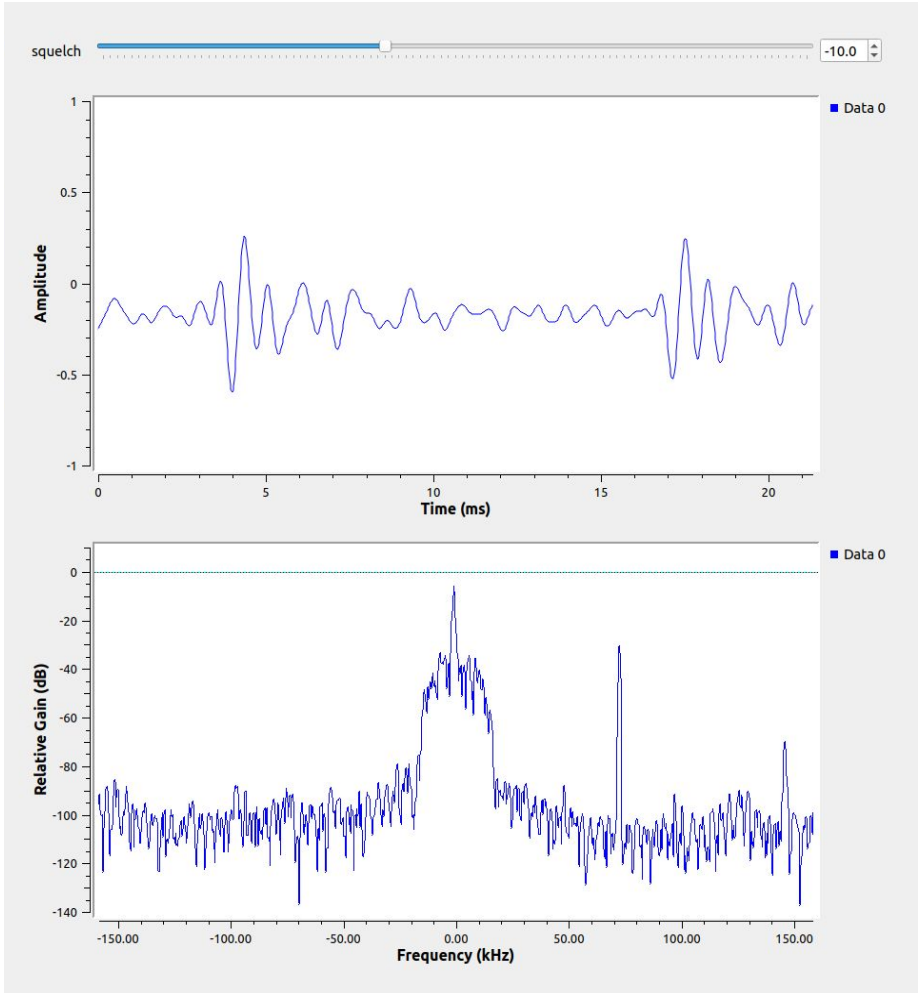
How it works



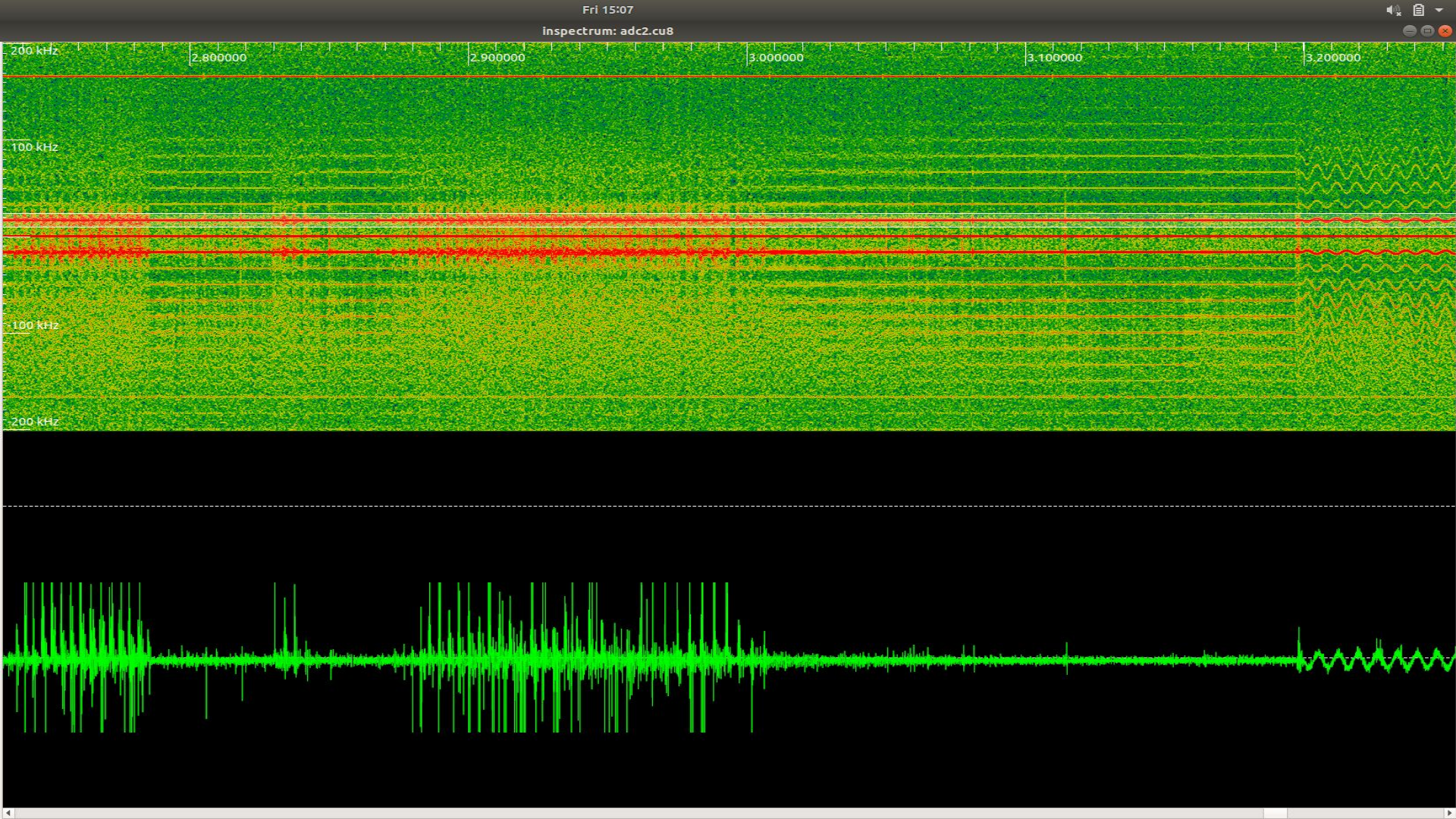


Breadboard SDR - FM Receiver





FM Breadboard Receiver


Fri 15:07
inspectrum: adc2.cu8
200 kHz
2.800000
2.900000
3.000000
3.100000
3.200000
100 kHz
-100 kHz
-200 kHz

When you build a radio in software, you don’t need much hardware

Scenario

We need to transmit data from our microcontroller project, but but don’t want to wait for RF modules to ship.

Can we program a microcontroller to transmit data over the air?

Clock Signal Transmitters

Toggling IO Pins

Miek’s OOK transmitter

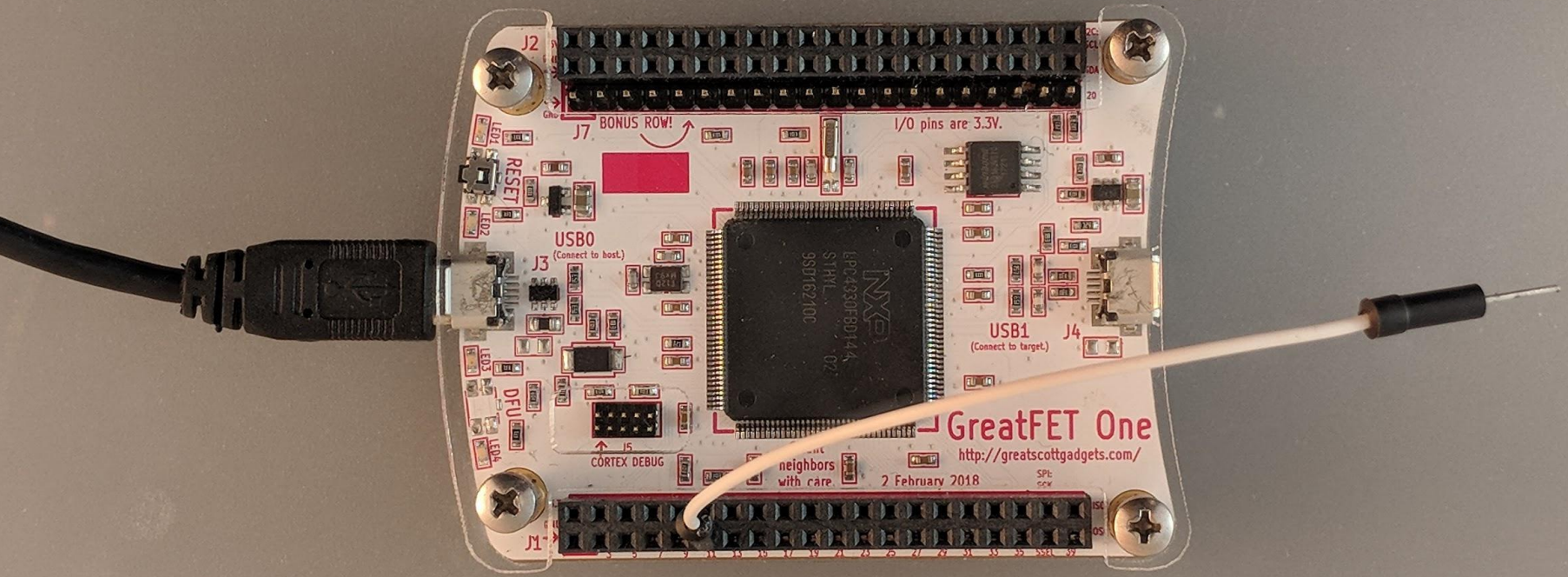
https://gfycat.com/gifs/detail/cloudyinfamouscapybara

Ang Cui’s Funtenna

http://www.funtenna.org/CuiBH2015.pdf

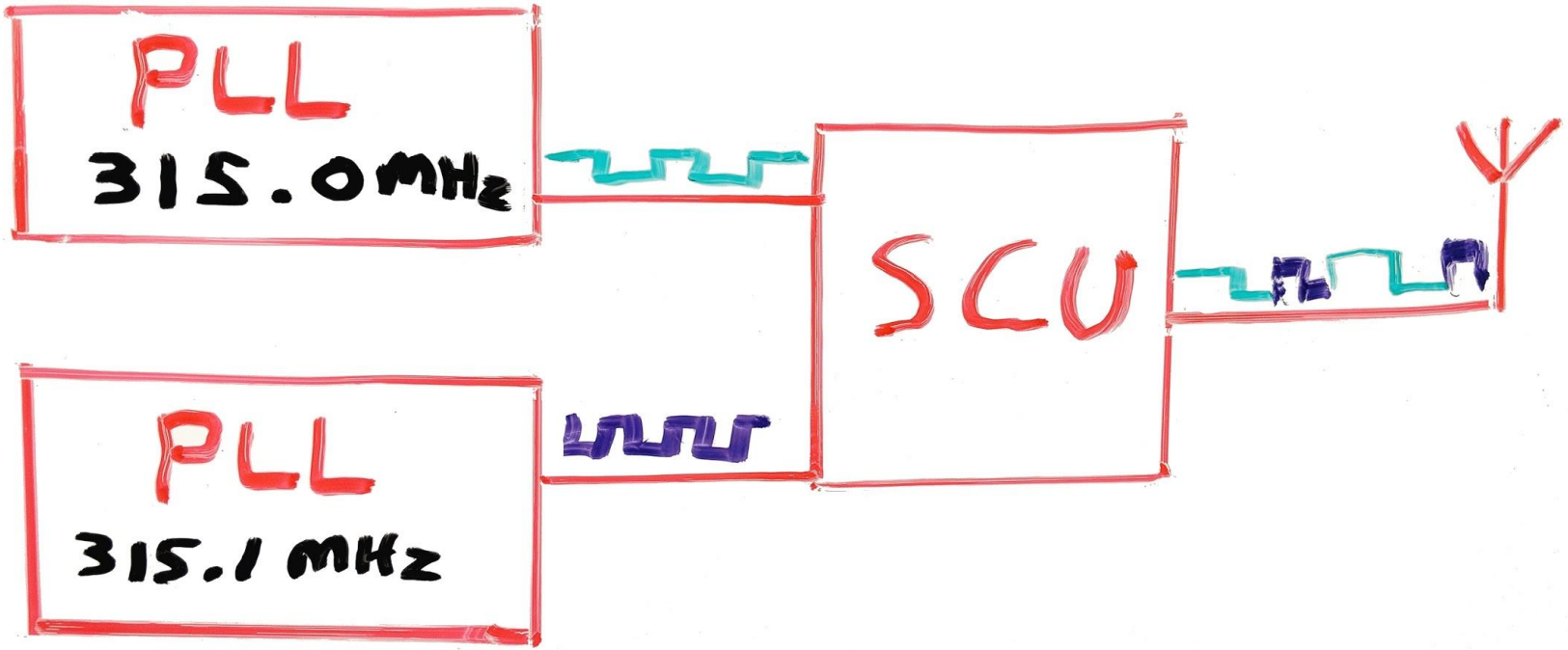
Raspberry Pi FM

https://github.com/PNPtutorials/FM_Transmitter_RPi3



GreatFET One PLL Transmitter

How it works



Real World Radios

Our demonstration target used a frequency deviation of +/-25 kHz and a center frequency of 315.005 MHz.

We transmitted with a frequency deviation of +/-50 kHz at a center frequency of 315.050 MHz, and it worked!

If it oscillates like a radio
and emits like a radio

It’s a radio

Scenario

Authoritarian governments restrict import/export of Analog to Digital Converters (ADC) in an effort to prevent distribution of technology.

Can we use a General-Purpose I/O (GPIO) pin on a microcontroller to implement a receiver without an ADC?

converters, electro-optical or "optical integrated circuits" designed for "signal processing", field programmable logic devices, custom integrated circuits for which either the function is unknown or the control status of the equipment in which the integrated circuit will be used in unknown, Fast Fourier Transform (FFT) processors, electrical erasable programmable read-only memories (EEPROMs), flash memories or static random-access memories (SRAMs), having any of the following:

a.2.a. Rated for operation at an ambient temperature above 398 K (+125°C);

a.2.b. Rated for operation at an ambient temperature below 218 K (-55°C); *or*

a.2.c. Rated for operation over the entire ambient temperature range from 218 K (-55°C) to 398 K (125°C);

a.5.a.2. A resolution of 10 bit or more, but less than 12 bit, with an output rate greater than 500 million words per second;

a.5.a.3. A resolution of 12 bit or more, but less than 14 bit, with an output rate greater than 200 million words per second;

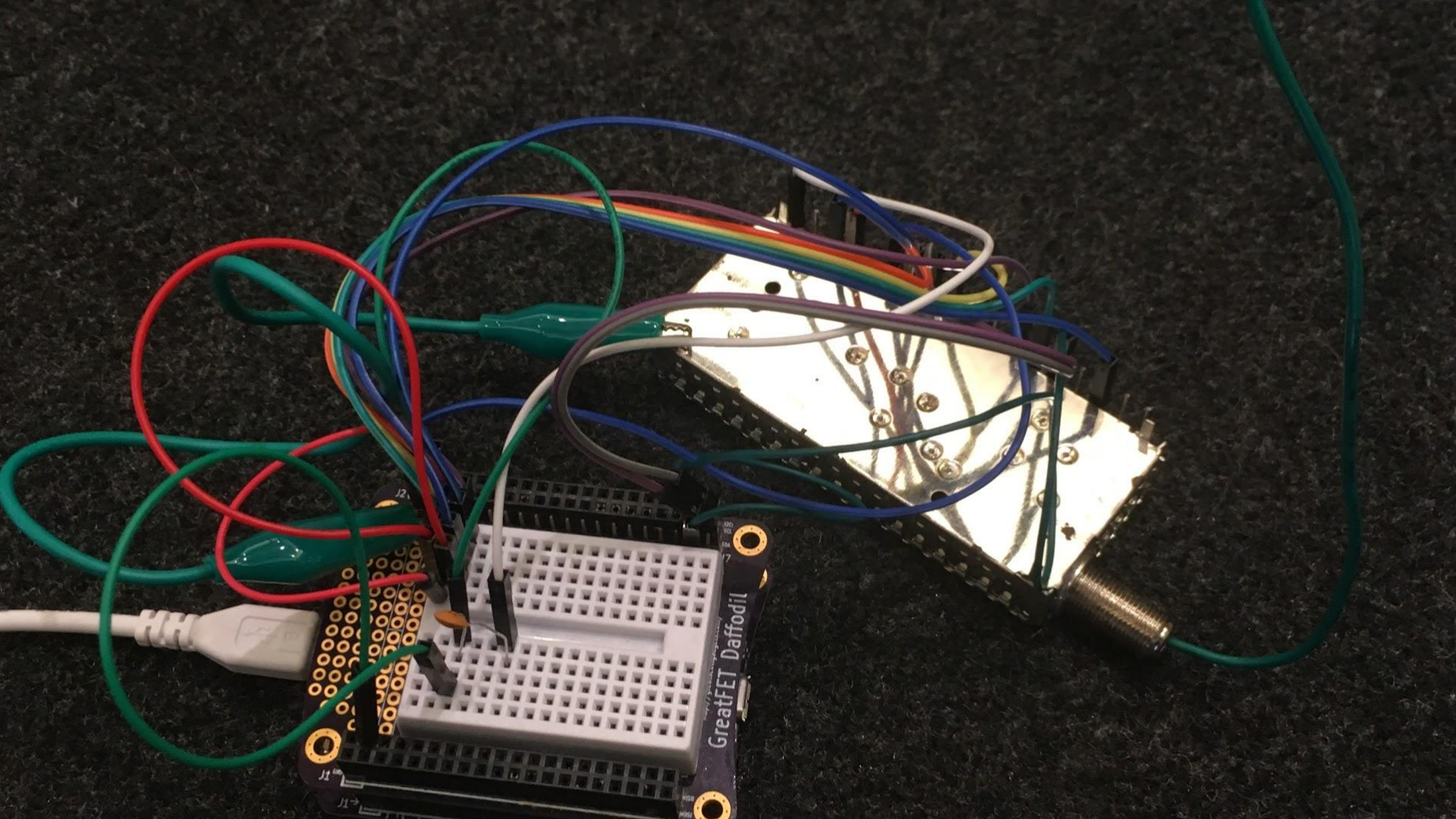
a.5.a.4. A resolution of 14 bit or more, but less than 16 bit, with an output rate greater than 250 million words per second; *or*

a.5.a.5. A resolution of 16 bit or more with an output rate greater than 65 million words per second;

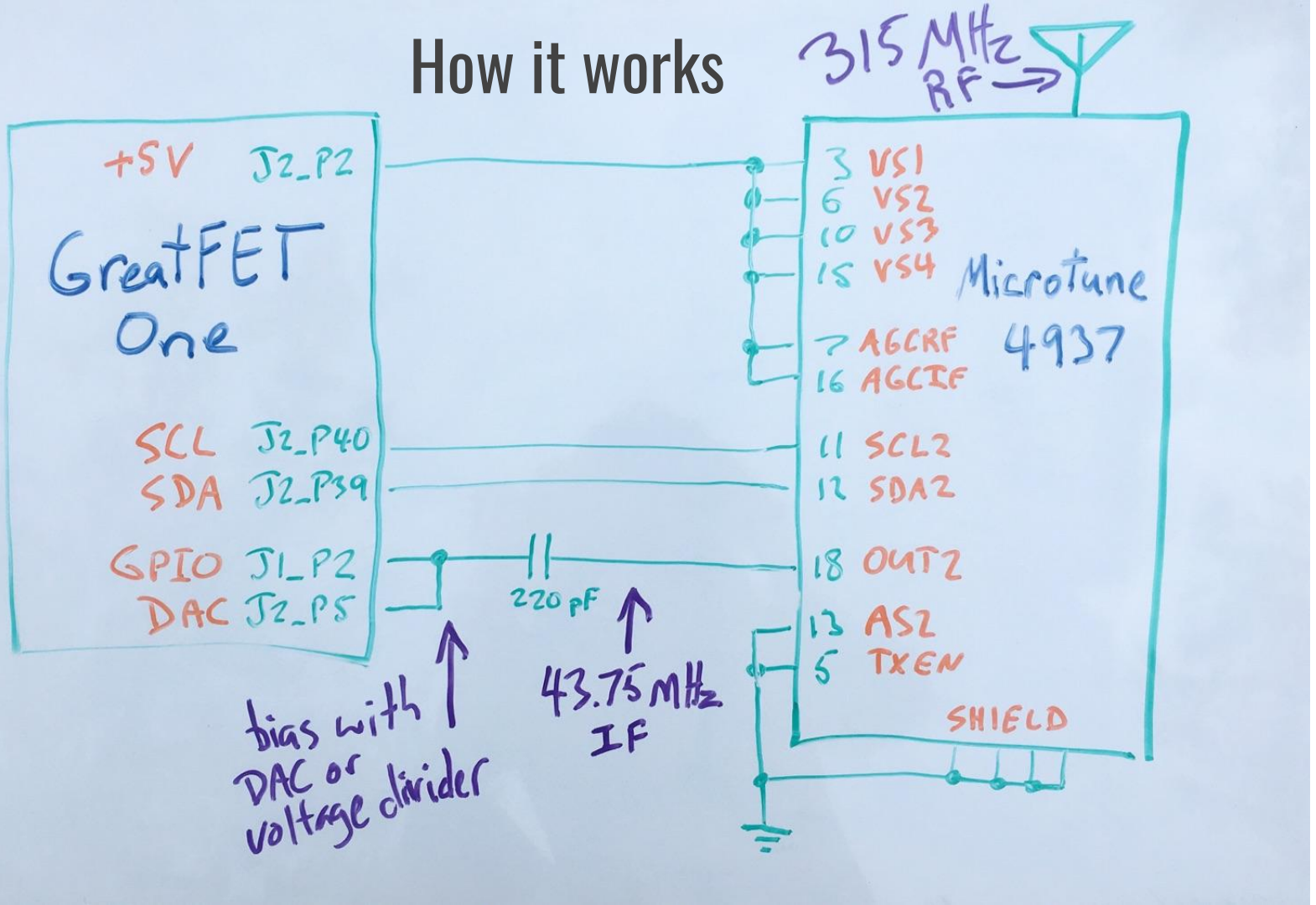
***Technical Notes*:**

1. A resolution of n bit corresponds to a quantization of 2^n levels.

GPIO Pin Receiver


GreatFET Daffodil

How it works


315 MHz RF
+5V J2_P2
GreatFET One
SCL J2_P40
SDA J2_P39
GPIO J1_P2
DAC J2_P5
220 pF
43.75 MHz IF
bias with DAC or voltage divider
3 VS1
6 VS2
10 VS3
15 VS4
7 AGCRF
16 AGCIF
Microtune 4937
11 SCL2
12 SDA2
18 OUT2
13 AS2
5 TXEN
SHIELD

Problems

The signal is at 43.75 MHz but we sample 25 MHz of bandwidth

We’re going to need more than 1 bit of dynamic range to recover signals

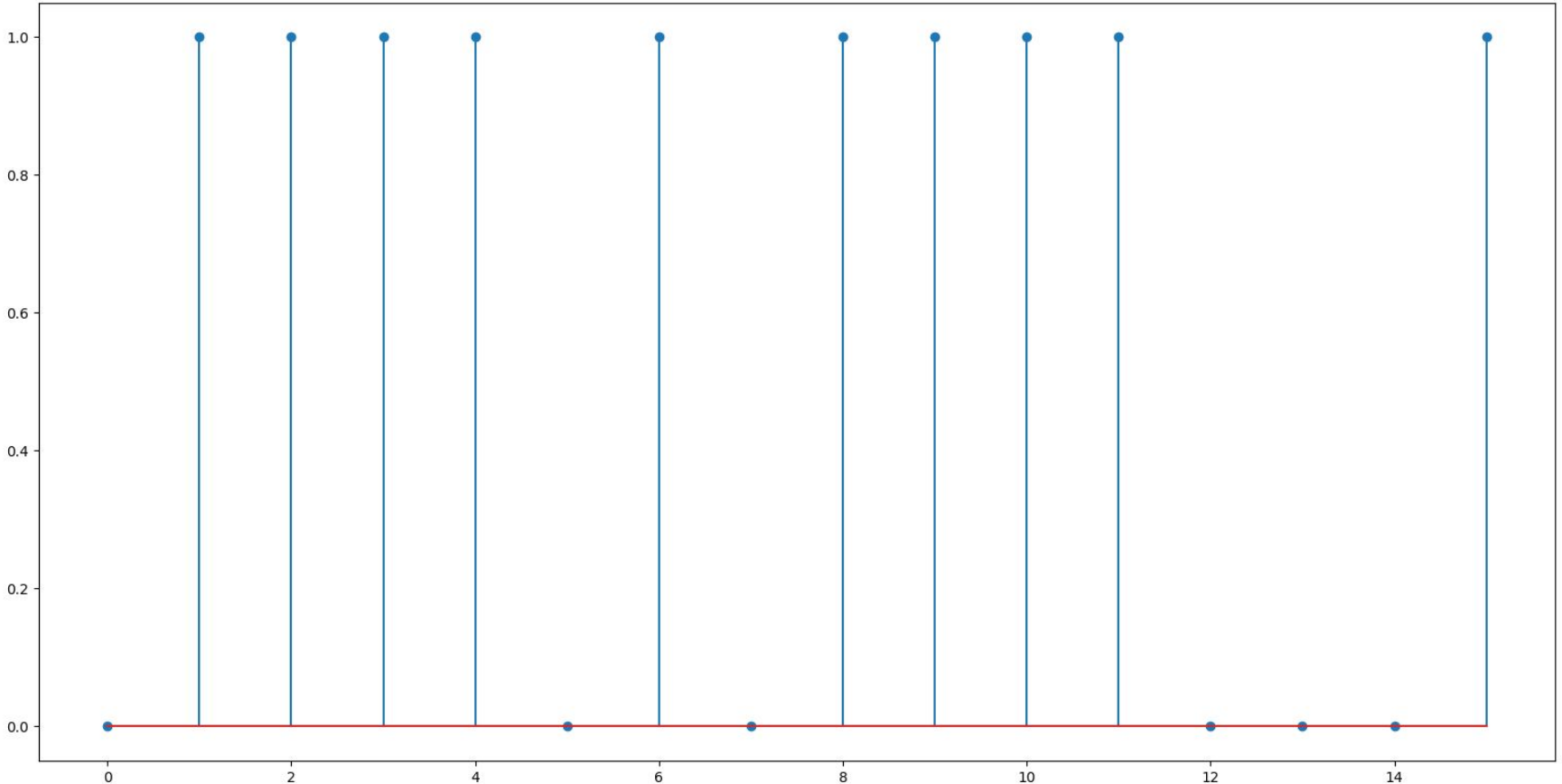
Undersampling

The signal is at 43.75 MHz

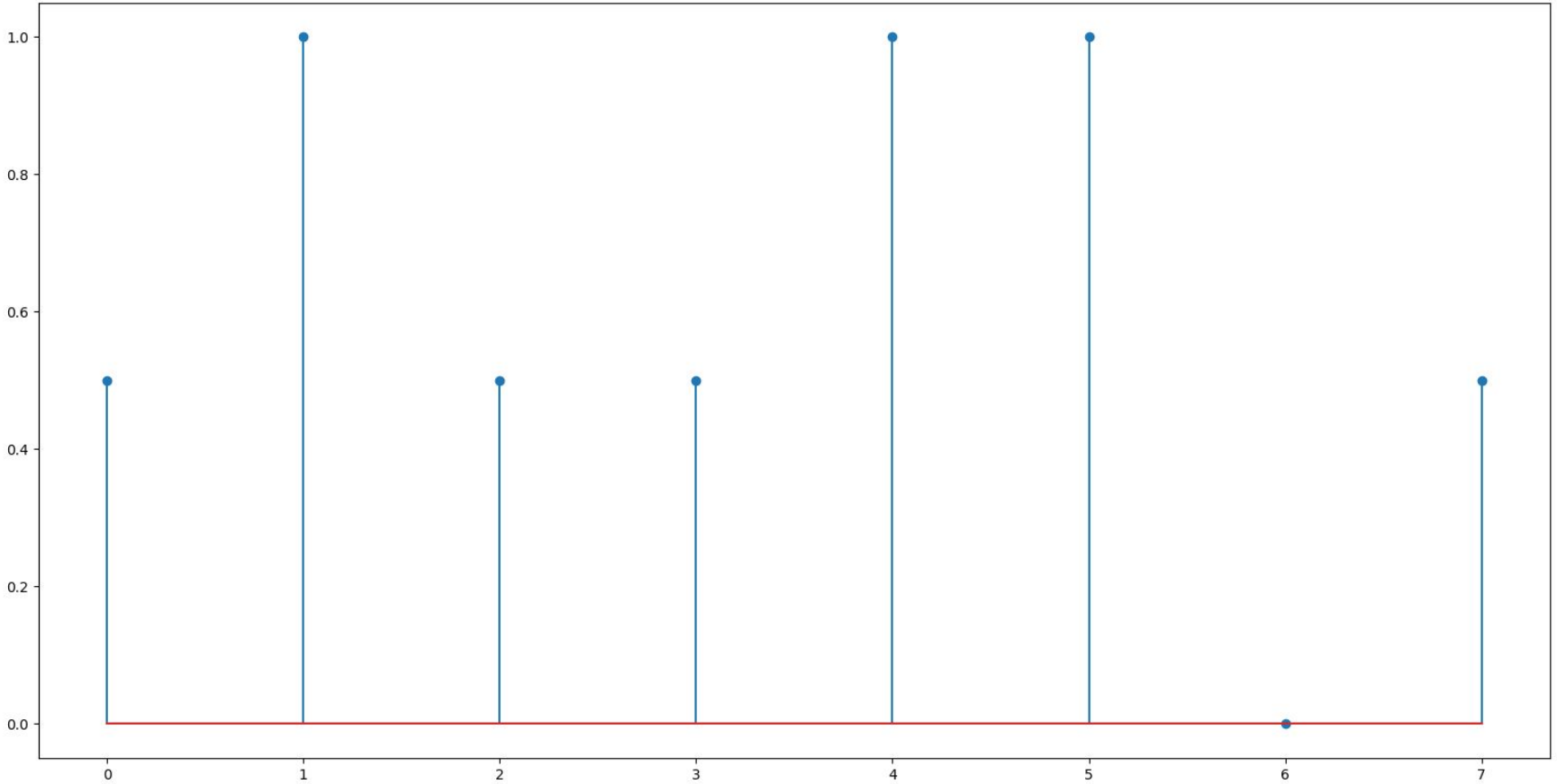
We sample at 50 MHz (25 MHz bandwidth)

We’ll see aliases, but we’ll try to ignore them

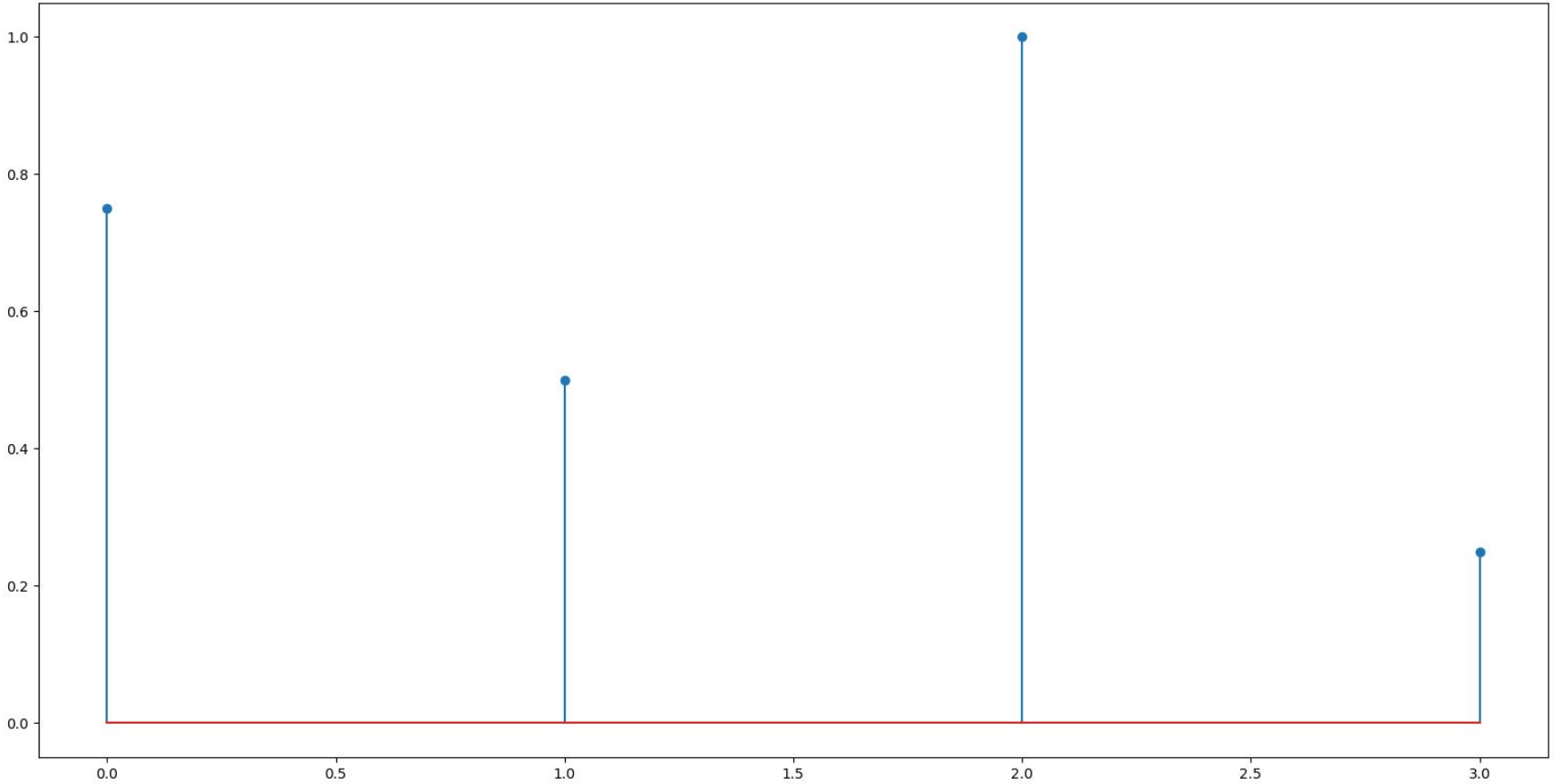
Oversample and Decimate



Oversample and Decimate

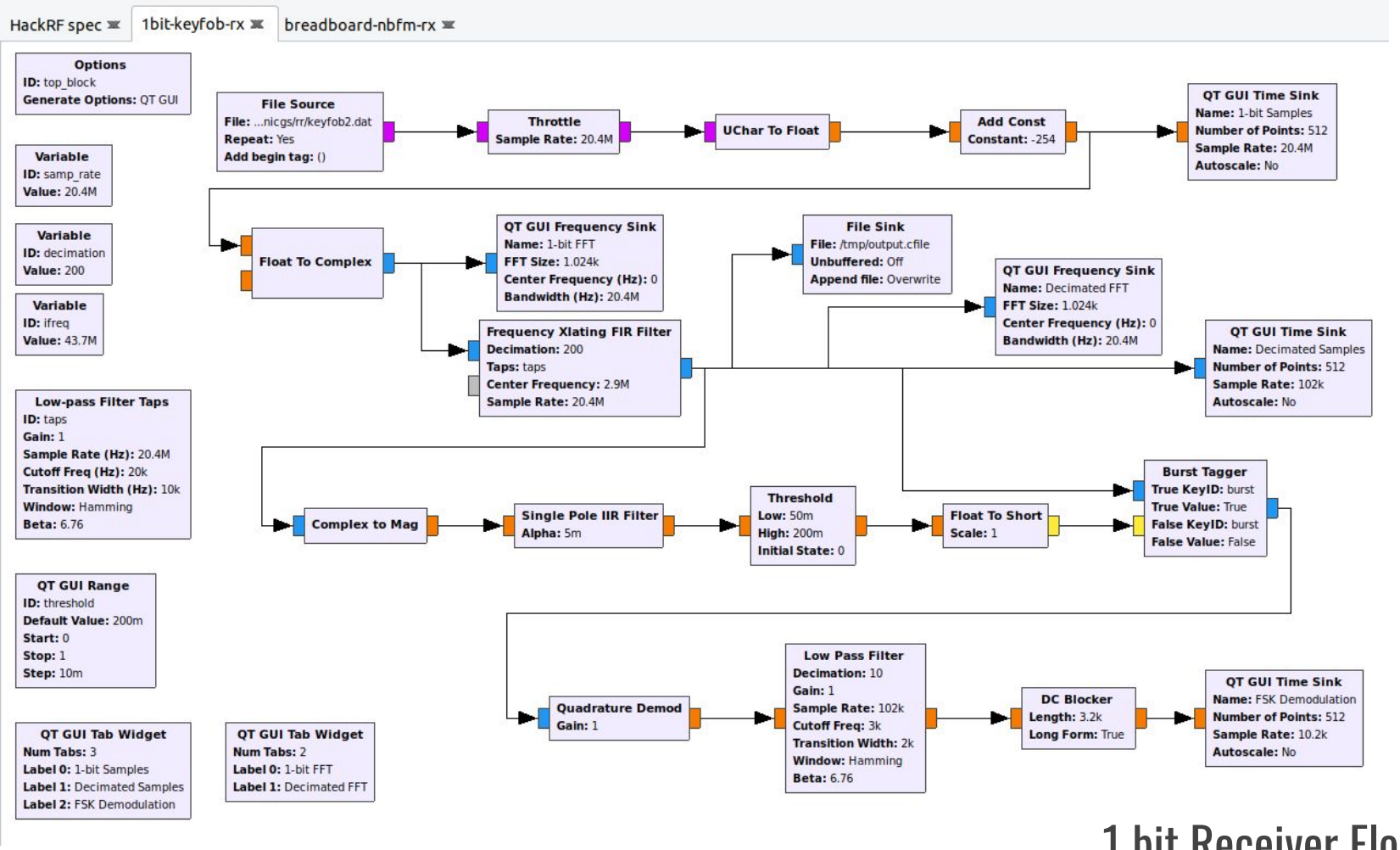


Oversample and Decimate

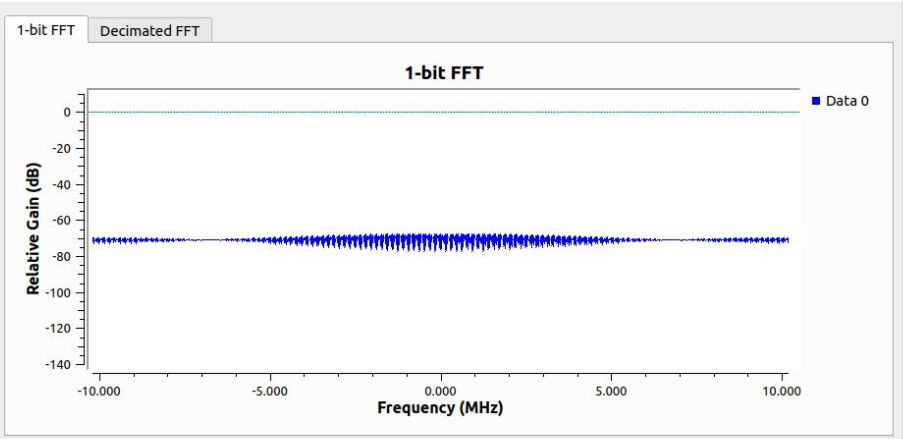


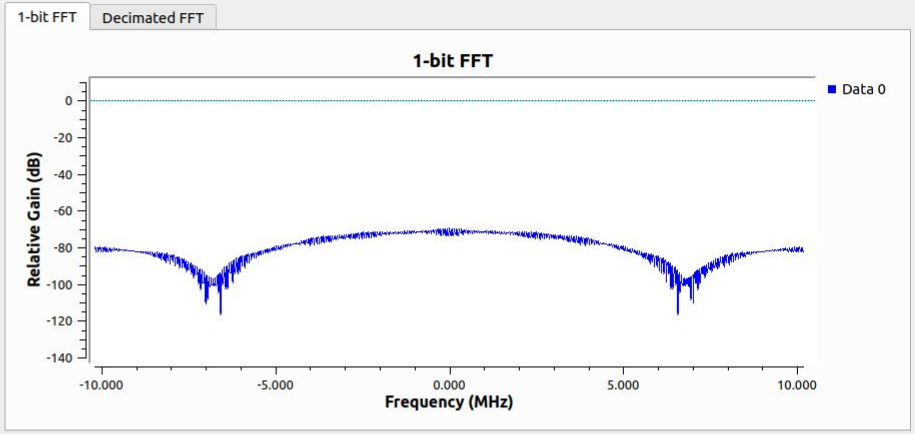
Oversampling and Undersampling

At the same time!

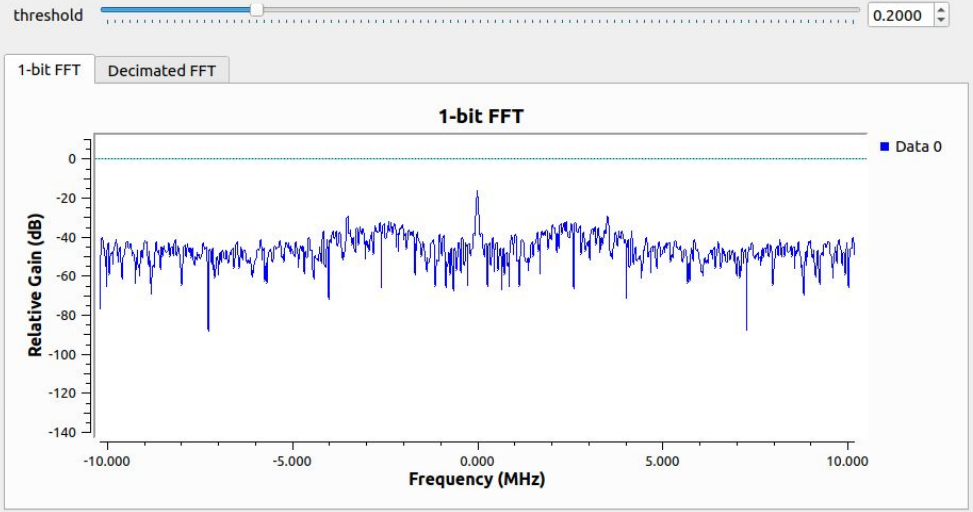


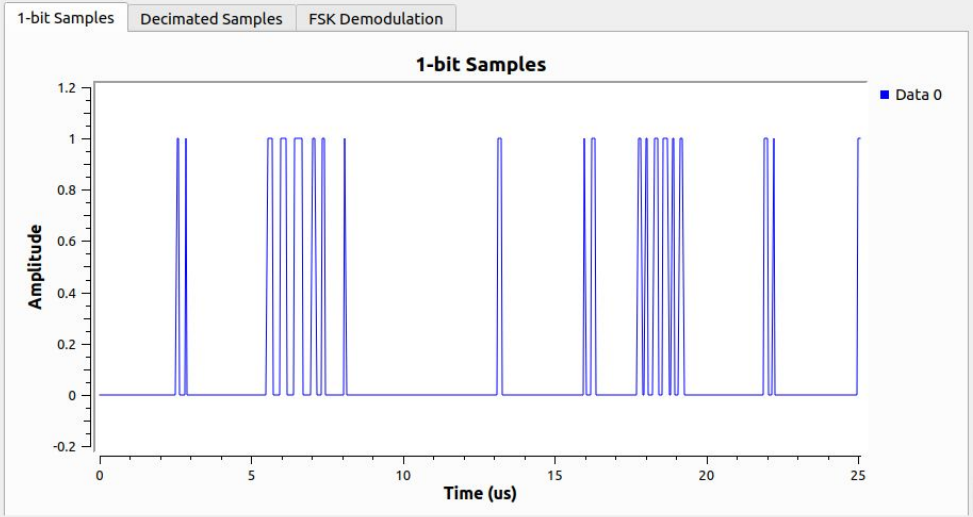
1 bit Receiver Flowgraph



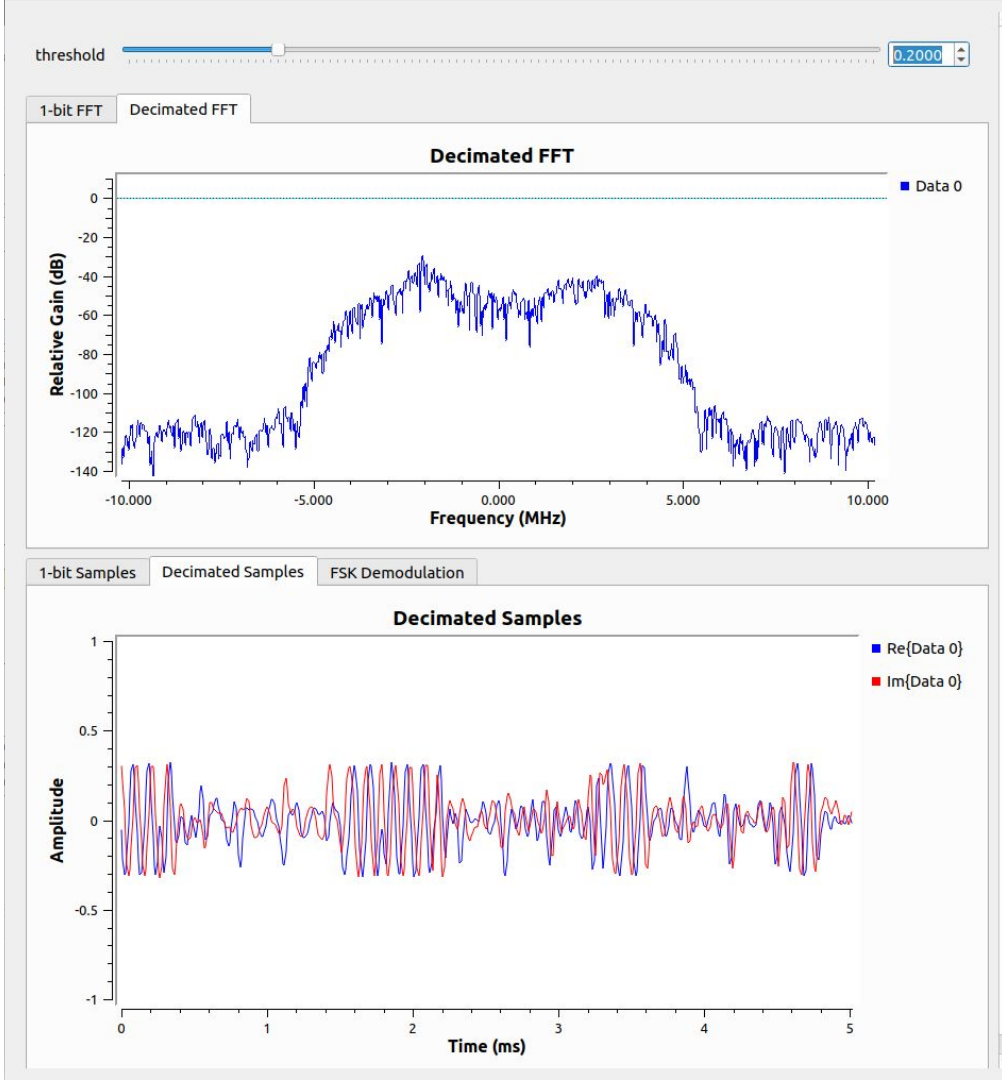


1 bit samples

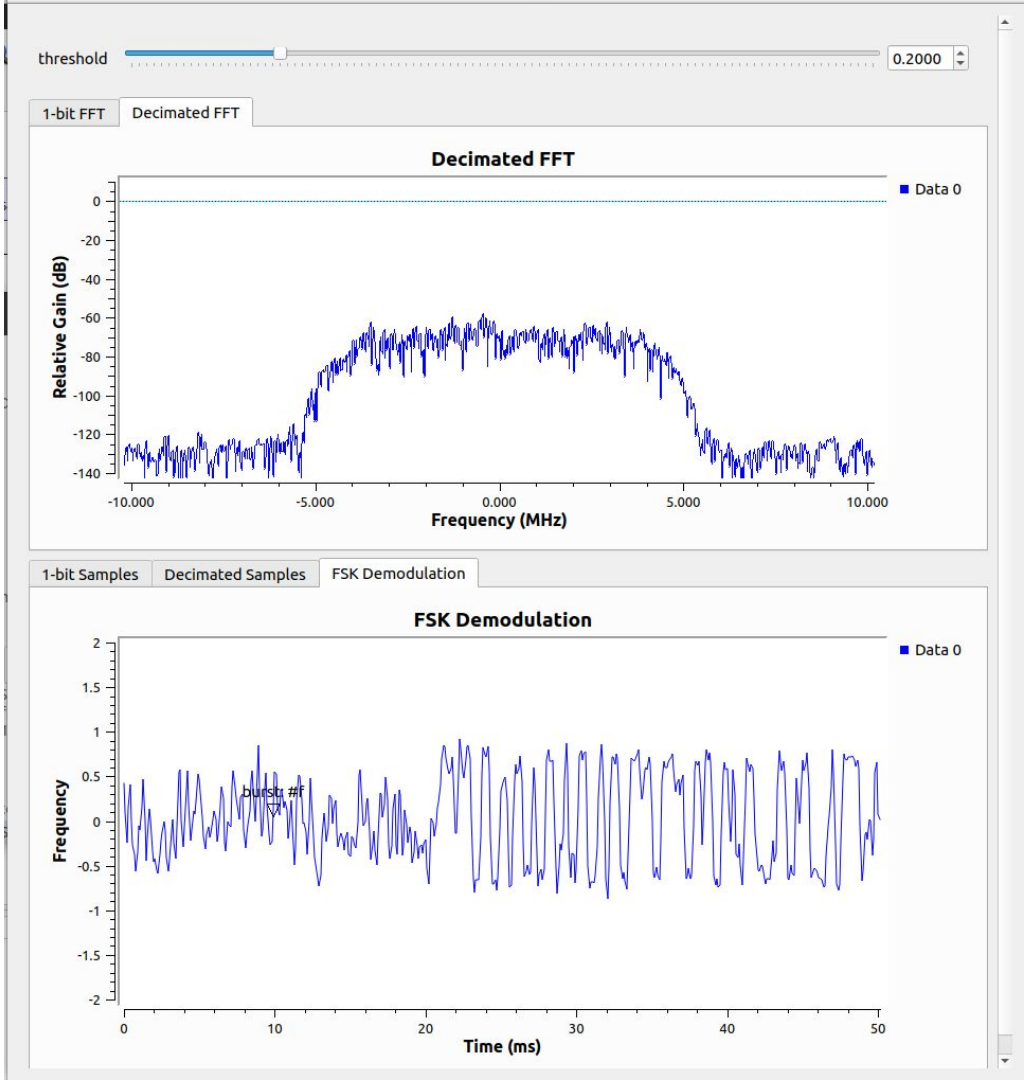




Oversample and decimate



FSK Demodulation



1 bit of dynamic range ought to be enough for anybody

Scenario

Big Brother (Mike Ossmann) has developed a pseudo-Doppler direction finder to track down illegal radio transmitters.

Can we steal a direction finder and use it as a direction finding countermeasure?

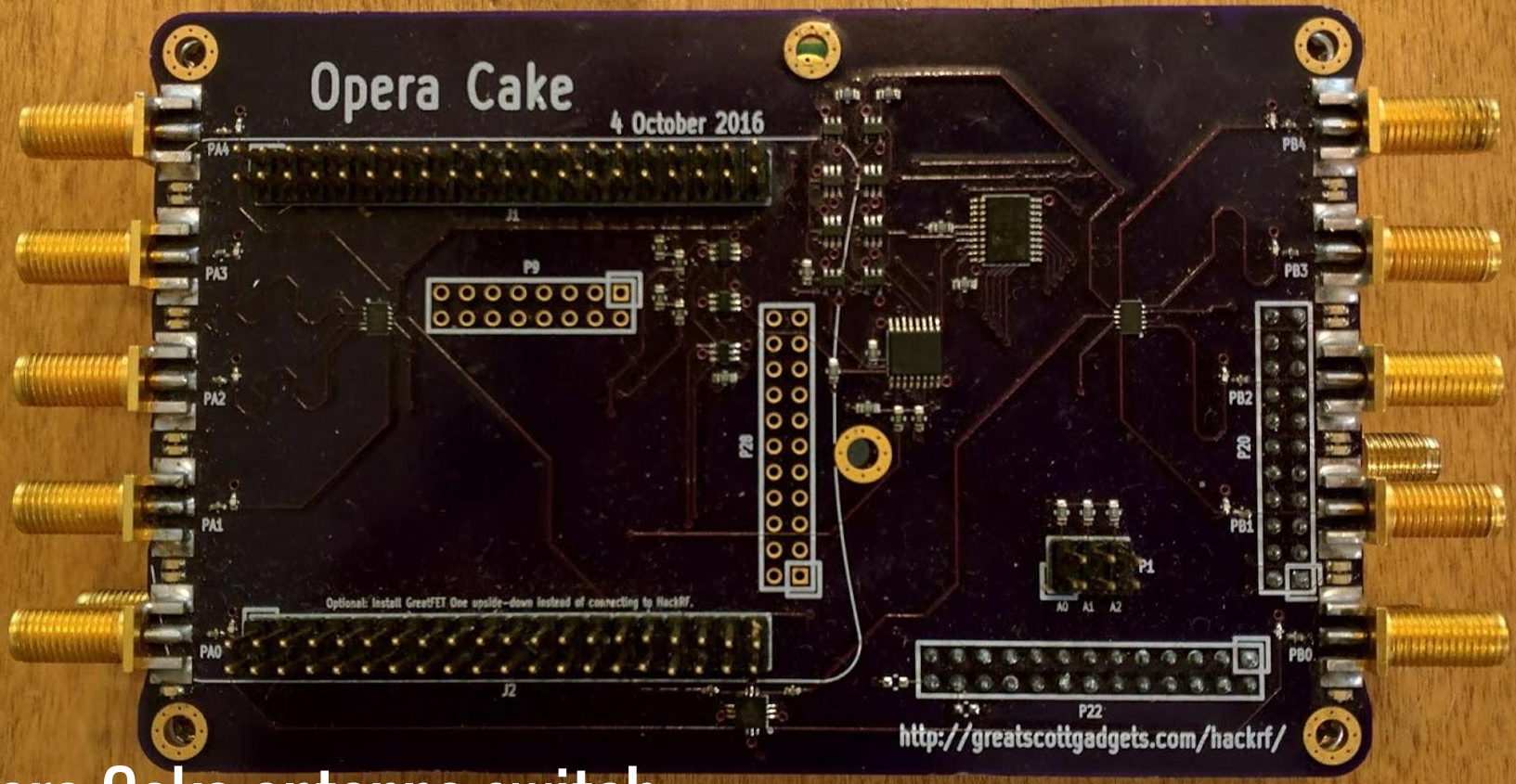
Direction finder to PSK transmitter

Pseudo-Doppler Direction Finding

Using an antenna switching board, we rapidly change antennas, introducing a doppler shift that reveals the direction of a transmitter.

Pseudo-Doppler Redux

Michael Ossmann and Schuyler St. Leger, Shmoocon 2018
https://archive.org/details/Shmoocon2018/Shmoocon2018-Pseudo-dopplerRedux.mp4



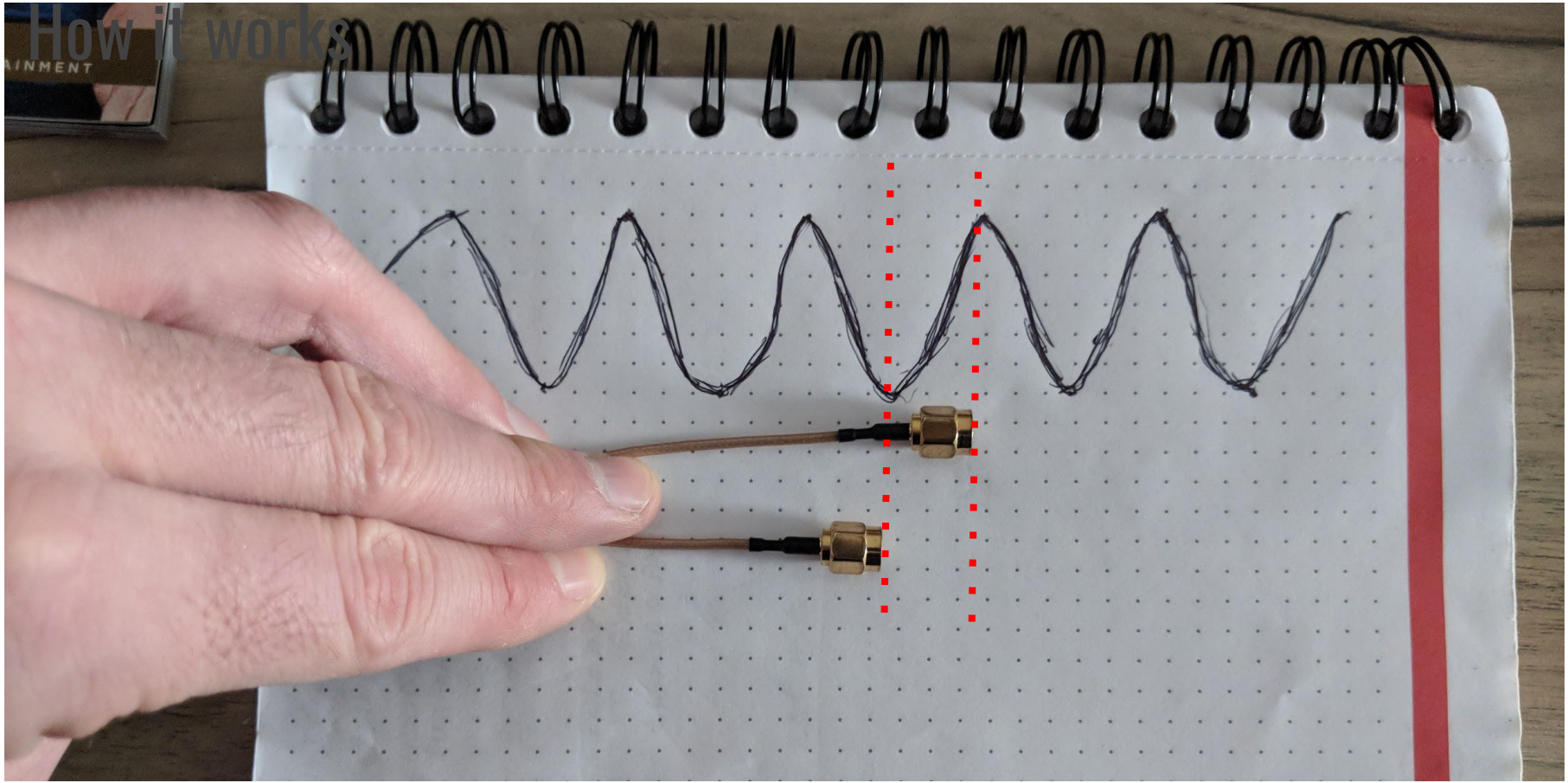
Opera Cake antenna switch

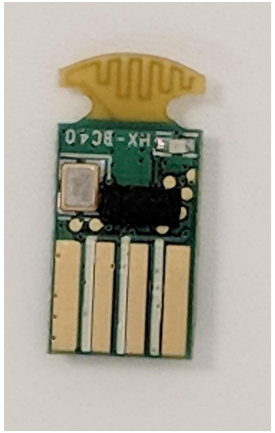
Phase shifting

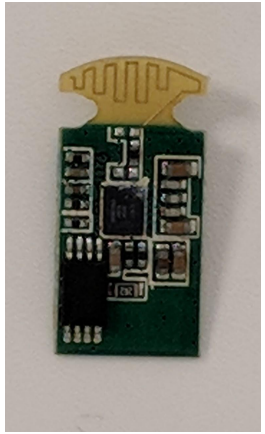
Switching between spatially distinct antennas introduces a phase shift

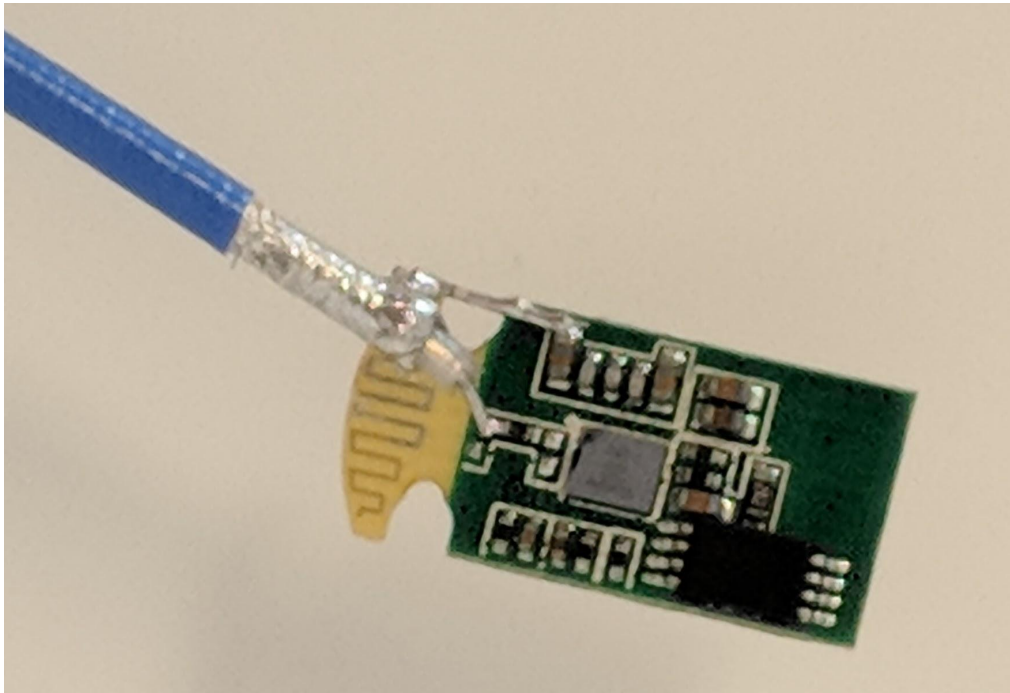
The same effect occurs if two lengths of cable are used

How it works

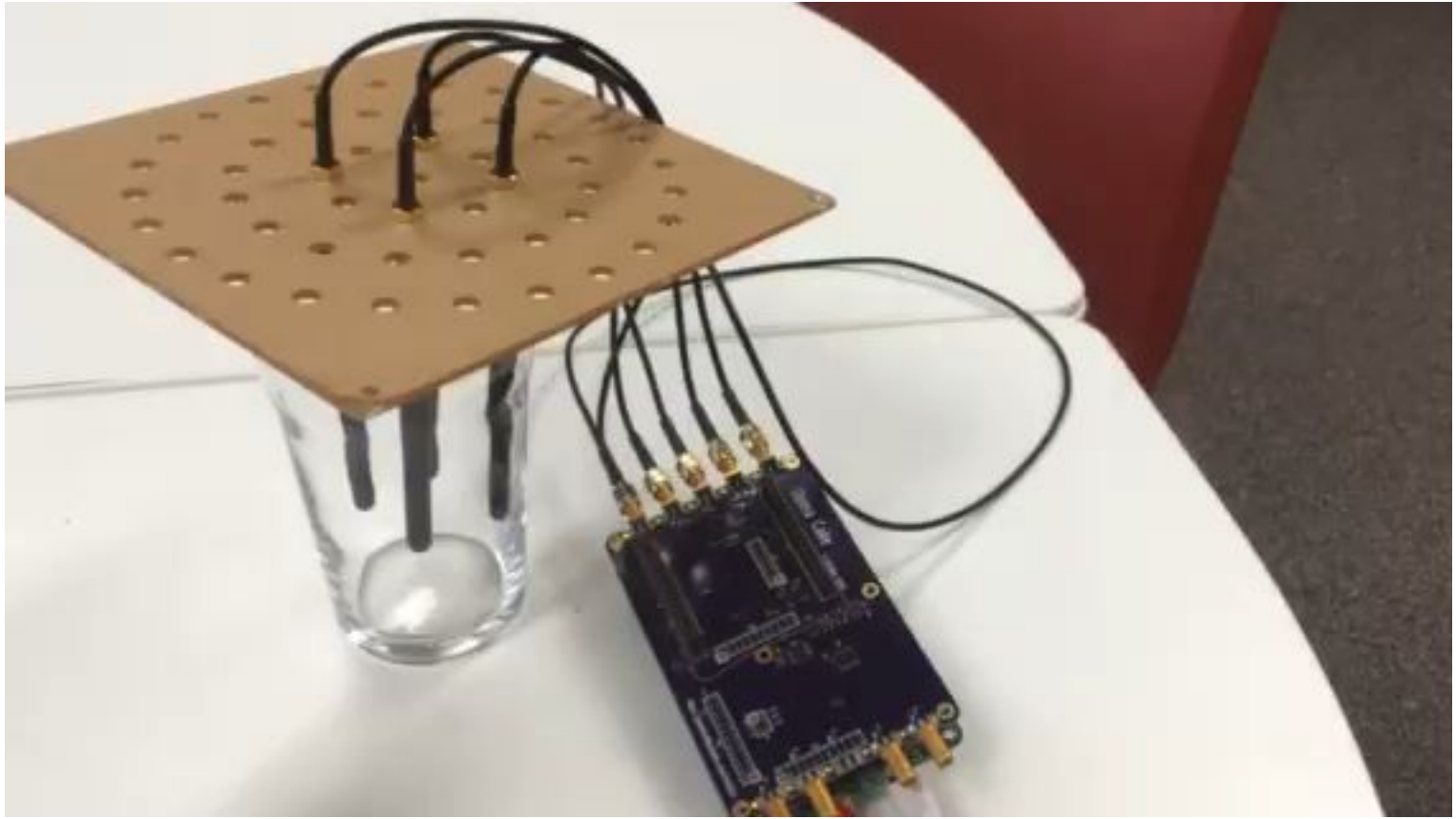








Cheap 2.4 GHz Source



Adding phase shifts circumvents pseudo-Doppler

Scenario

Since we can affect the phase, can we use a direction finder to implement a Phase Shift-Keying (PSK) transmitter?

Covert Channels

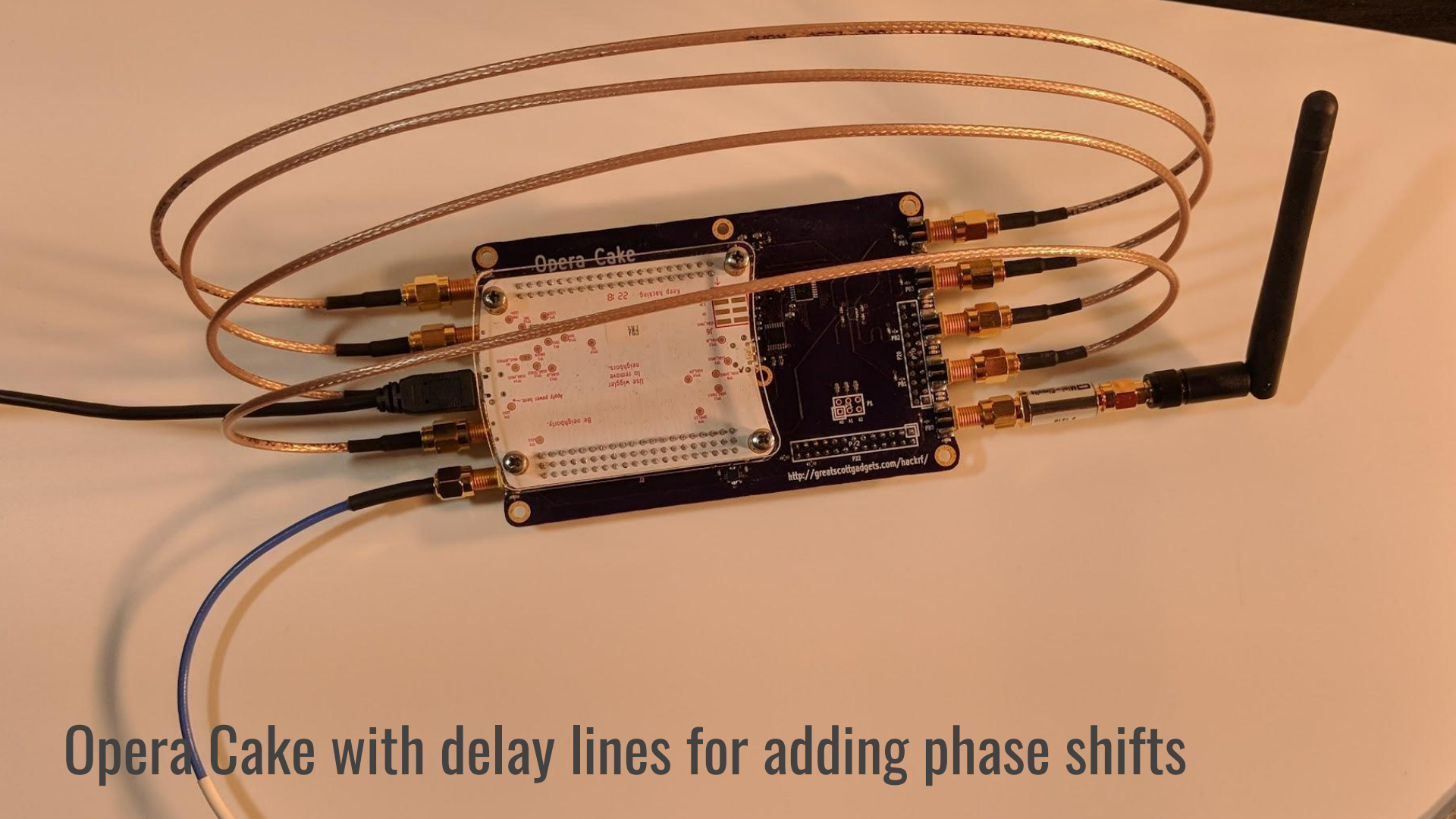
A Protocol for Leibowitz

Travis Goodspeed and Sergey Bratus, REcon 2015
http://www.cs.dartmouth.edu/~sergey/phy/leibowitz-recon2015.pdf

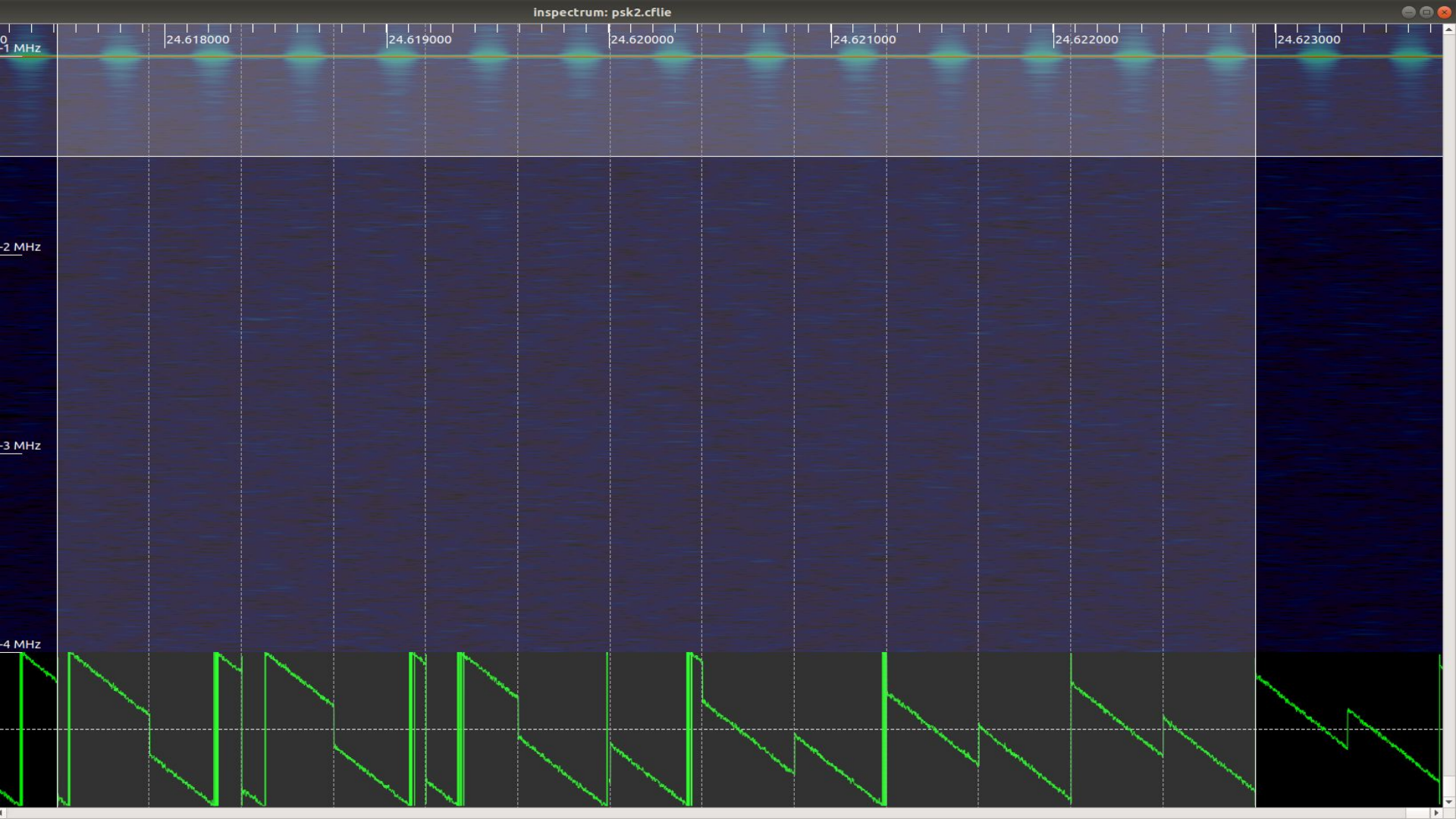
Fillory of PHY: Toward a Periodic Table of Signal Corruption Exploits and Polyglots in Digital Radio

Sergey Bratus, Travis Goodspeed, Ange Albertini, Debanjum S. Solanky, WOOT 2016

http://www.cs.dartmouth.edu/~sergey/phy/leibowitz-recon2015.pdf



Opera Cake with delay lines for adding phase shifts

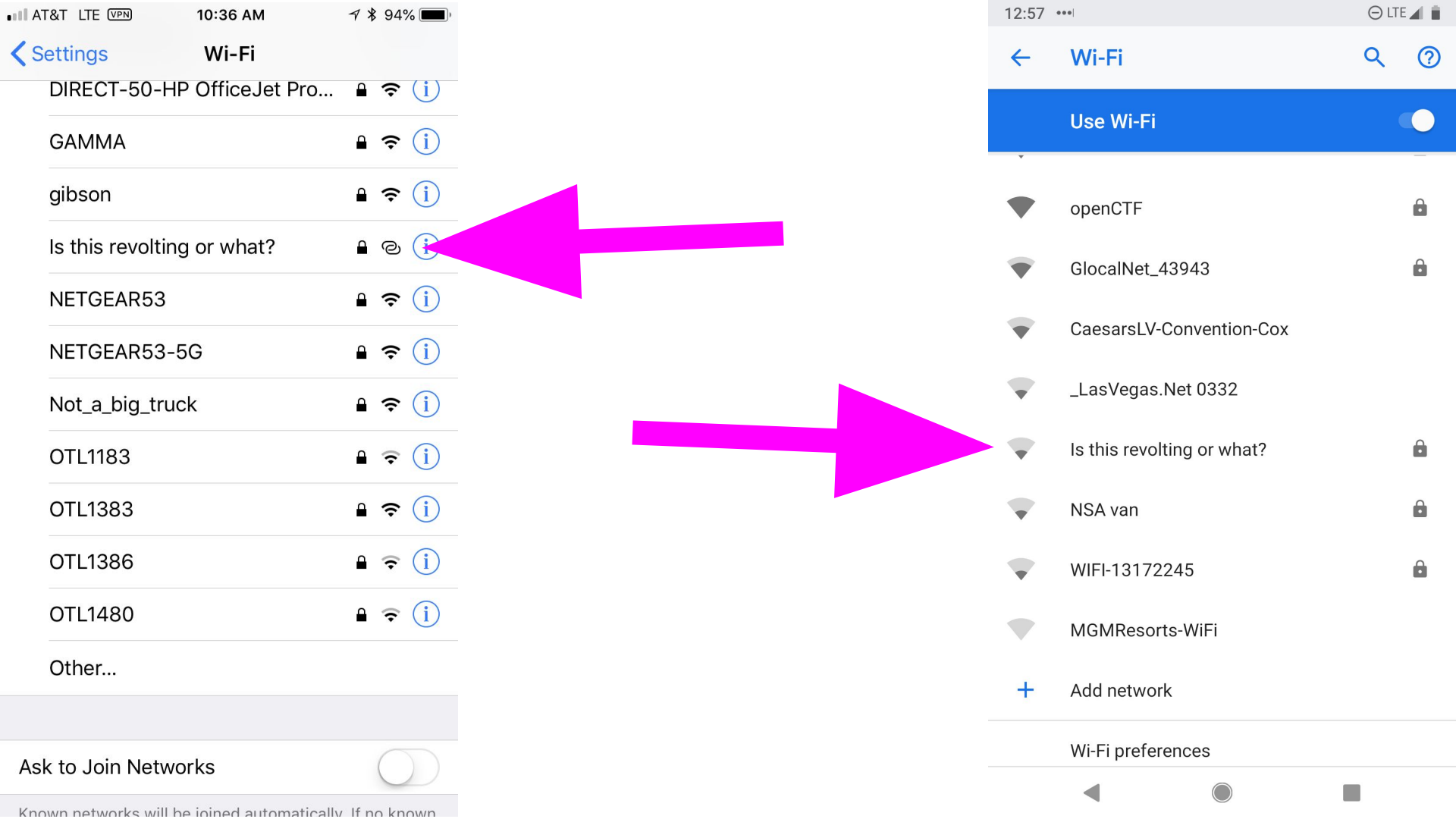

inspectrum: psk2.cflie
24.618000
24.619000
24.620000
24.621000
24.622000
24.623000
-1 MHz
-2 MHz
-3 MHz
-4 MHz

How it works

2.4 GHz PSK

Paths can be switched at >11 MHz

DSSS is just fast PSK


AT&T LTE VPN
10:36 AM
94%
Settings
Wi-Fi
DIRECT-50-HP OfficeJet Pro...
GAMMA
gibson
Is this revolting or what?
NETGEAR53
NETGEAR53-5G
Not_a_big_truck
OTL1183
OTL1383
OTL1386
OTL1480
Other...
Ask to Join Networks
Known networks will be joined automatically. If no known
12:57
LTE
Wi-Fi
Use Wi-Fi
openCTF
GlocalNet_43943
CaesarsLV-Convention-Cox
_LasVegas.Net 0332
Is this revolting or what?
NSA van
WIFI-13172245
MGMResorts-WiFi
Add network
Wi-Fi preferences

An external modulator can add a covert channel

Thanks

Mike Walters

Ang Cui

Schuyler St. Leger

Matt Ettus

Jared Boone

Root Killah

Sergey Bratus

Travis Goodspeed

Taylor Streetman

Jacob Graves

Piotr Esden-Tempski

Michael Ossmann

References

---

https://github.com/greatscottgadgets/greatfet

https://github.com/mossmann/hackrf

Find us on Twitter: @dominicgs / @michaelossmann