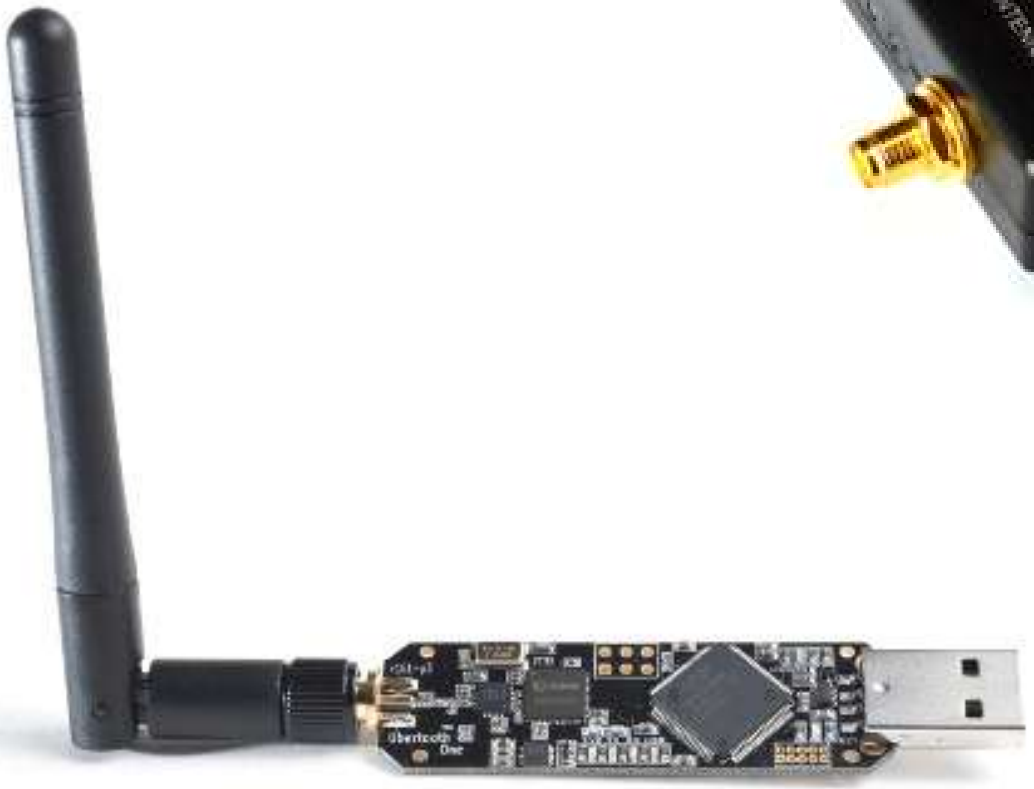
NSA Playset: RF Retroreflectors

Michael Ossmann
Great Scott Gadgets


GREAT SCOTT GADGETS™
Throwing Star LAN Tap Pro™


HackRF One
GREAT SCOTT GADGETS




C1
220pF
Throwing Star LAN Tap
r2-p2
C2
220pF
J4

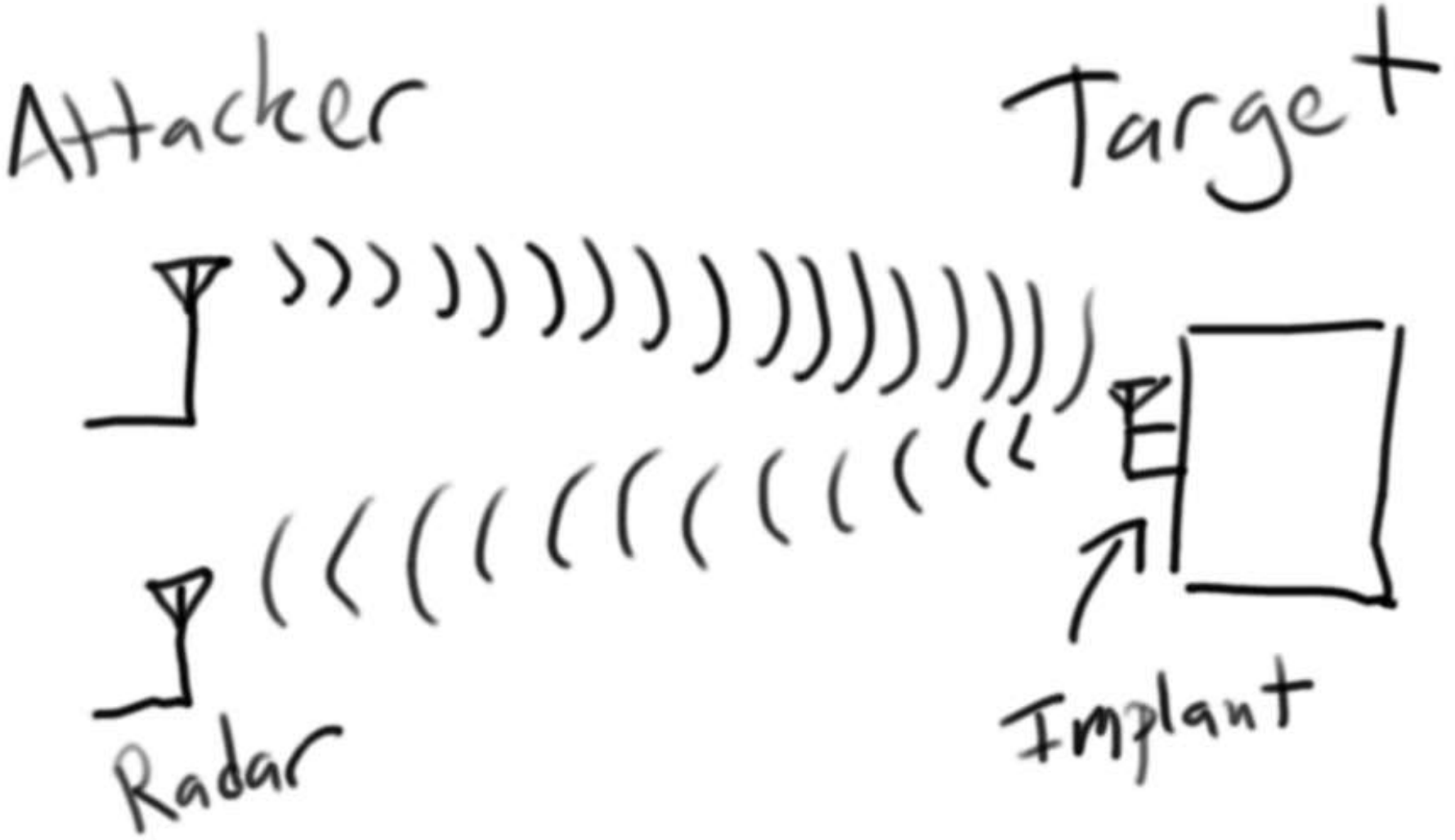
The NSA Playset

Play along with the NSA!

Ossmann & Pierce, ToorCamp 2014:

http://ossmann.blogspot.com/2014/07/the-nsa-playset.html

RF Retroreflectors



not reverse engineering

What to Expect

Leaked classified information
(NSA ANT catalog)

My hardware designs

How to build your own retroreflectors

Live demonstration

and...

The State of Emission Security

active attacks

vs.

passive attacks

Passive Attacks

unintentional emissions

Code name: TEMPEST

plenty of research

e.g. Markus Kuhn

Active Attacks

The Thing

(Great Seal Bug)

RAGEMASTER

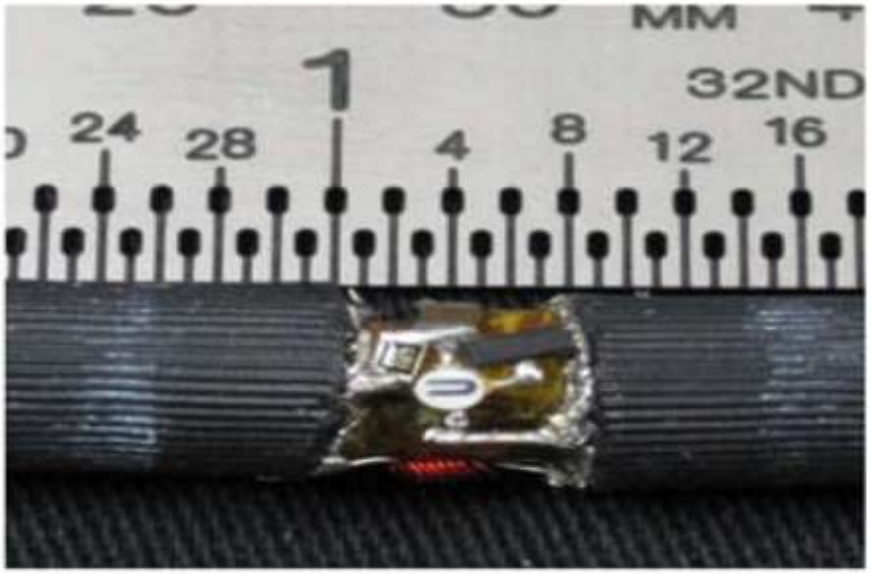
ANT Product Data

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

24 Jul 2008

(U) Capabilities

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.



CTX4000

ANT Product Data

(TS//SI//REL TO USA,FVEY) The CTX4000 is a portable continuous wave (CW) radar unit. It can be used to illuminate a target system to recover different off net information. Primary uses include VAGRANT and DROPMIRE collection.

8 Jul 2008

(TS//SI//REL TO USA,FVEY) The CTX4000 provides the means to collect signals that otherwise would not be collectable, or would be extremely difficult to collect and process. It provides the following features:

- Frequency Range: 1 - 2 GHz.
- Bandwidth: Up to 45 MHz
- Output Power: User adjustable up to 2 W using the internal amplifier; external amplifiers make it possible to go up to 1 kW.

NIGHTWATCH

ANT Product Data

(TS//SI//REL TO USA,FVEY) NIGHTWATCH is a portable computer with specialized, internal hardware designed to process progressive-scan (non-interlaced) VAGRANT signals.

24 Jul 2008

(U) Capability Summary

(TS//SI//REL TO USA,FVEY) The current implementation of NIGHTWATCH consists of a general-purpose PC inside of a shielded case. The PC has PCI digitizing and clock cards to provide the needed interface and accurate clocking required for video reconstruction. It also has:

- horizontal sync, vertical sync and video outputs to drive an external, multi-sync monitor.
- video input
- spectral analysis up to 150 kHz to provide for indications of horizontal and vertical sync frequencies
- frame capture and forwarding
- PCMCIA cards for program and data storage
- horizontal sync locking to keep the display set on the NIGHTWATCH display.
- frame averaging up to 2^16 (65536) frames.

SURLYSPAWN

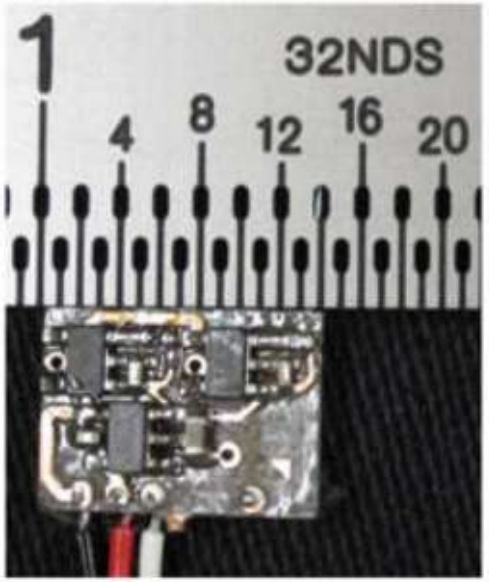
ANT Product Data

07 Apr 2009

(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.

(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,

TAWDRYYARD

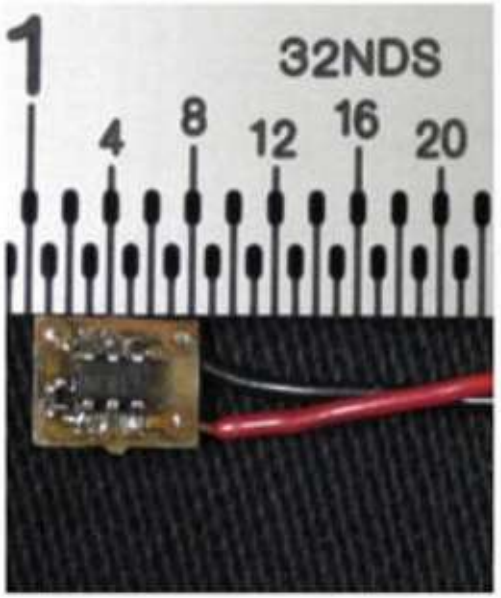
ANT Product Data

(TS//SI//REL TO USA,FVEY) Beacon RF retro-reflector. Provides return when illuminated with radar to provide rough positional location.

07 Apr 2009

(U) Capabilities

(TS//SI//REL TO USA,FVEY) TAWDRYYARD is used as a beacon, typically to assist in locating and identifying deployed RAGEMASTER units. Current design allows it to be detected and located quite easily within a 50' radius of the radar system being used to illuminate it. TAWDRYYARD draws as 8 µA at 2.5V (20µW) allowing a standard lithium coin cell to power it for months or years. The simplicity of the design allows the form factor to be tailored for specific operational requirements. Future capabilities being considered are return of GPS coordinates and a unique target identifier and automatic processing to scan a target area for presence of TAWDRYYARDs. All components are COTS and so are non-attributable to NSA.



(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The board generates a square wave operating at a preset frequency. This square wave is used to turn a FET (field effect

LOUDAUTO

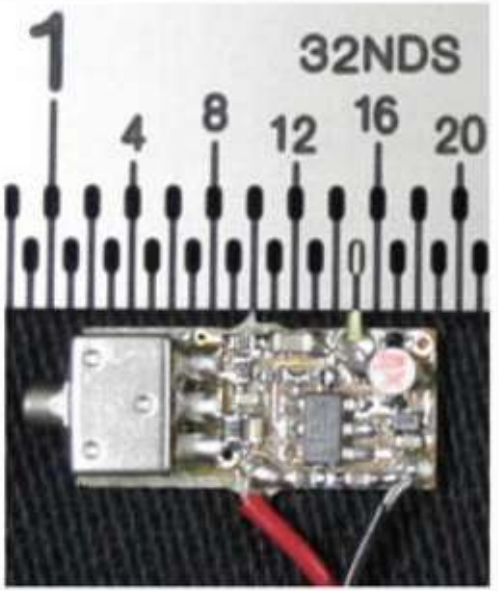
ANT Product Data

07 Apr 2009

(TS//SI//REL TO USA,FVEY) Audio-based RF retro-reflector. Provides room audio from targeted space using radar and basic post-processing.

(U) Capabilities

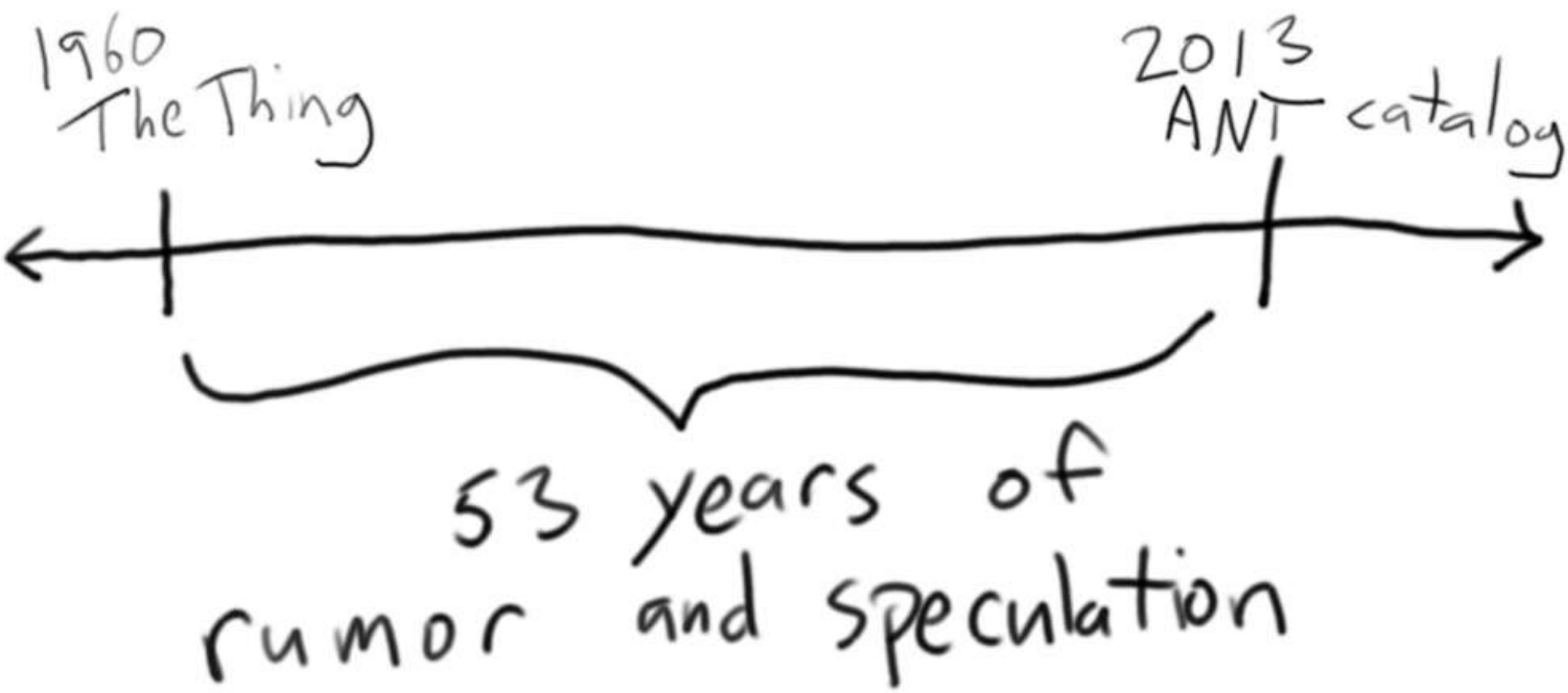
(TS//SI//REL TO USA,FVEY) LOUDAUTO's current design maximizes the gain of the microphone. This makes it extremely useful for picking up room audio. It can pick up speech at a standard, office volume from over 20' away. (NOTE: Concealments may reduce this distance.) It uses very little power (~15 uA at 3.0 VDC), so little, in fact, that battery self-discharge is more of an issue for serviceable lifetime than the power draw from this unit. The simplicity of the design allows the form factor to be tailored for specific operational requirements. All components at COTS and so are non-attributable to NSA.



(U) Concept of Operation

TS//SI//REL TO USA,FVEY) Room audio is picked up by the microphone and converted into an analog electrical signal. This signal is used to pulse position modulate (PPM) a square wave signal running at a pre-set frequency. This square wave is used to turn a FET (field effect transistor) on and off. When the unit is illuminated with a CW signal from a nearby radar unit, the illuminating signal is amplitude-modulated with the PPM square wave. This

A History of Active RF Emission Security



some
say
otherwise


PoC
or
GTFO

one brief mention in the literature

"irradiate it with this frequency and then detect keypress codes in the retransmitted signal"

Soft Tempest, Kuhn and Anderson

post-ANT catalog

one experimenter on YouTube: GBPPR

"retro-reflector"

or

"retroreflector"

RF Backscatter Communication

well researched

Communication by Means of Reflected Power

Harry Stockman, 1948

lots of more recent research

especially UHF RFID

Which Radar?

off-the shelf radar gear?

police radar typically >20 GHz

Hot Wheels Radar Gun!

Hot Wheels Radar Gun

often on Ebay for $25

often broken, but RF board almost always works

easy to add baseband output!

http://www.edparadis.com/radar

10 GHz

similar radar available as inexpensive module

(search for Arduino radar on Ebay)

Coffee Can Radar

Dr. Gregory Charvat and friends

2.4 GHz :)

typically used with low bandwidth sound card

:(

open source hardware FTW

HackRF One

Software Defined Radio (SDR) peripheral

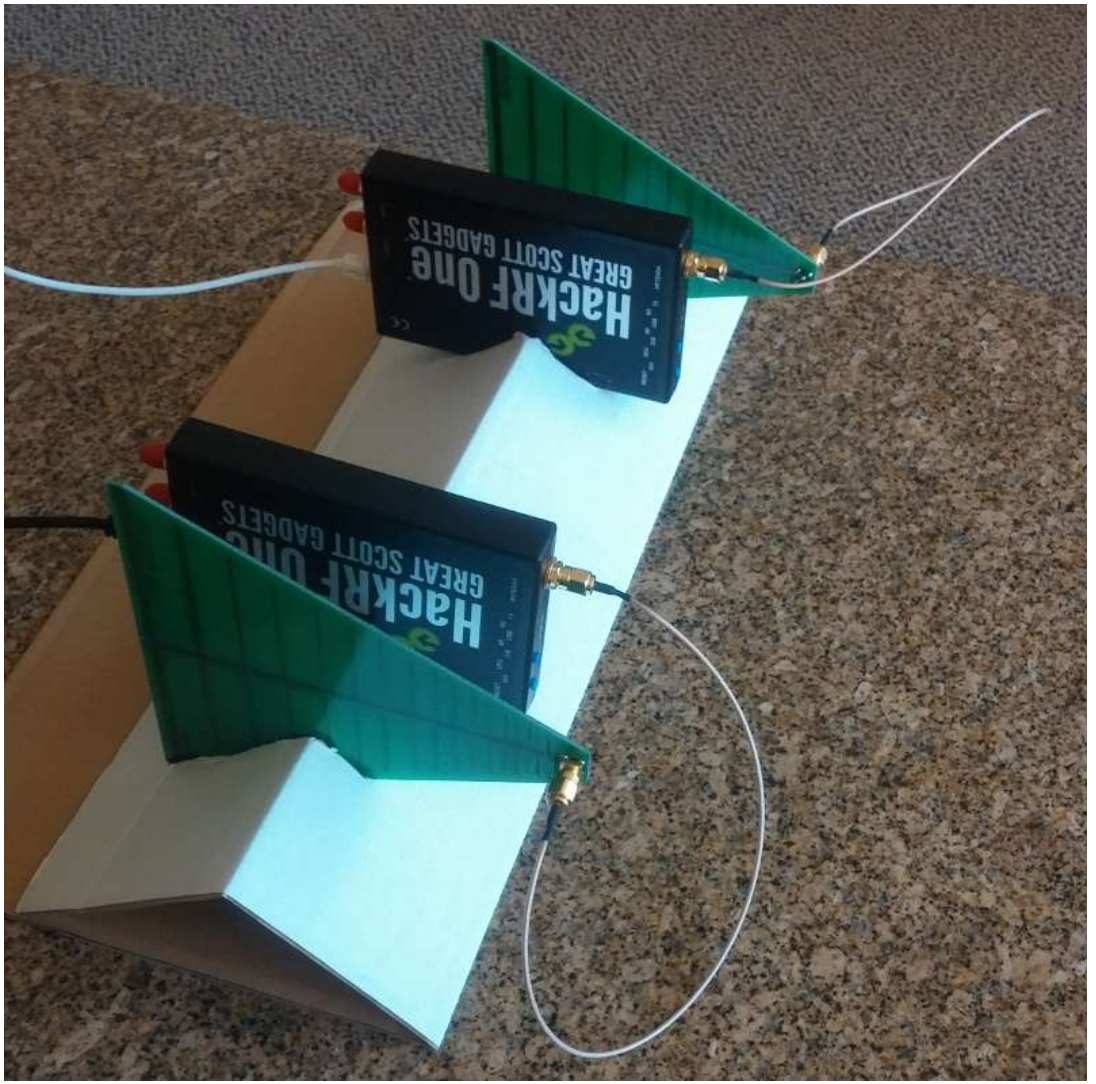
Open source hardware

official frequency range: 10 MHz - 6 GHz

20 MHz bandwidth

half-duplex transceiver

HackRF Radar



antenna by Kent Britain (WA5VJB)

2482 MHz

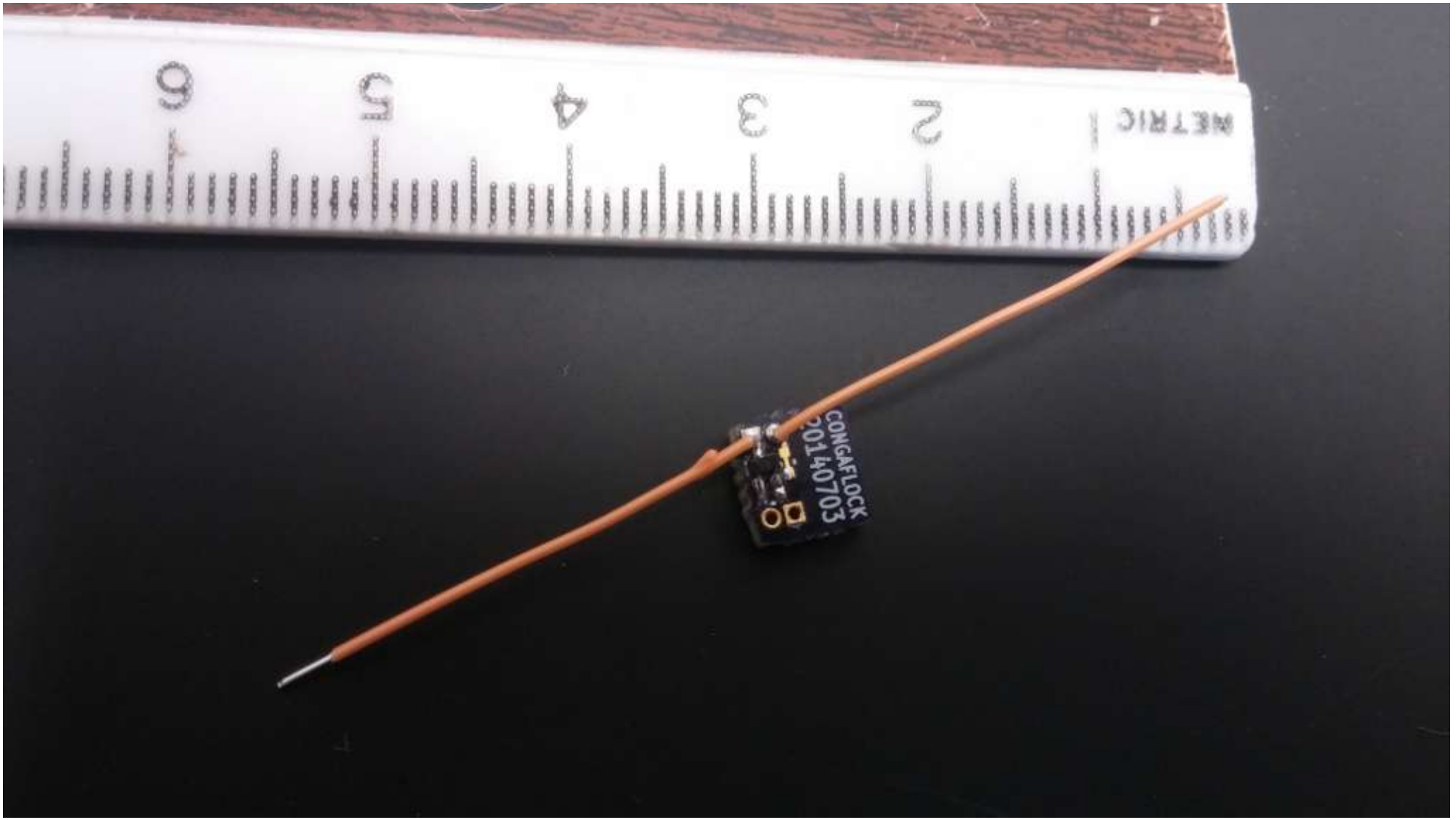
NSA uses 1 GHz to 4 GHz

2.4 GHz ISM band
(but higher than Wi-Fi and Bluetooth)

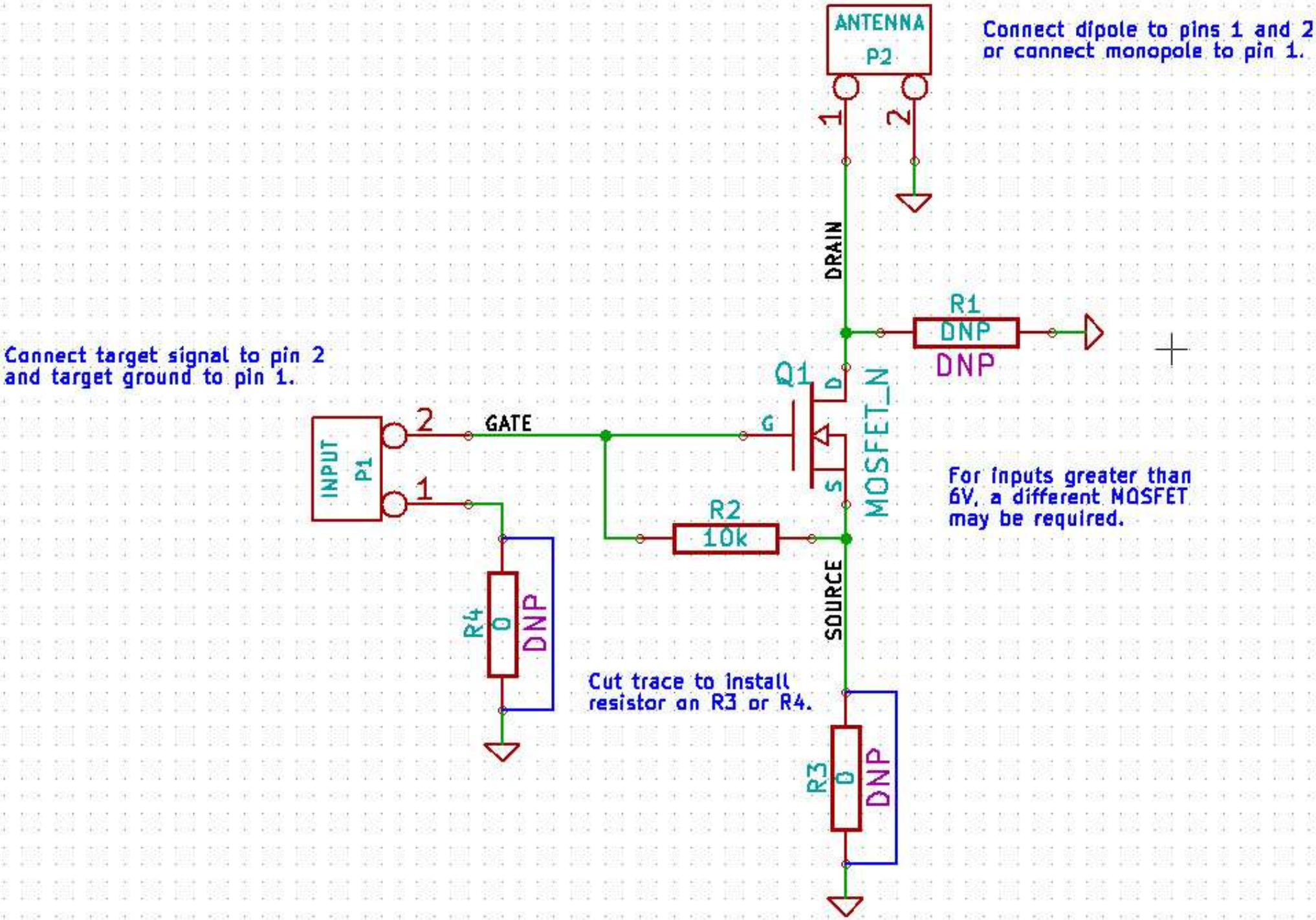
best HackRF performance

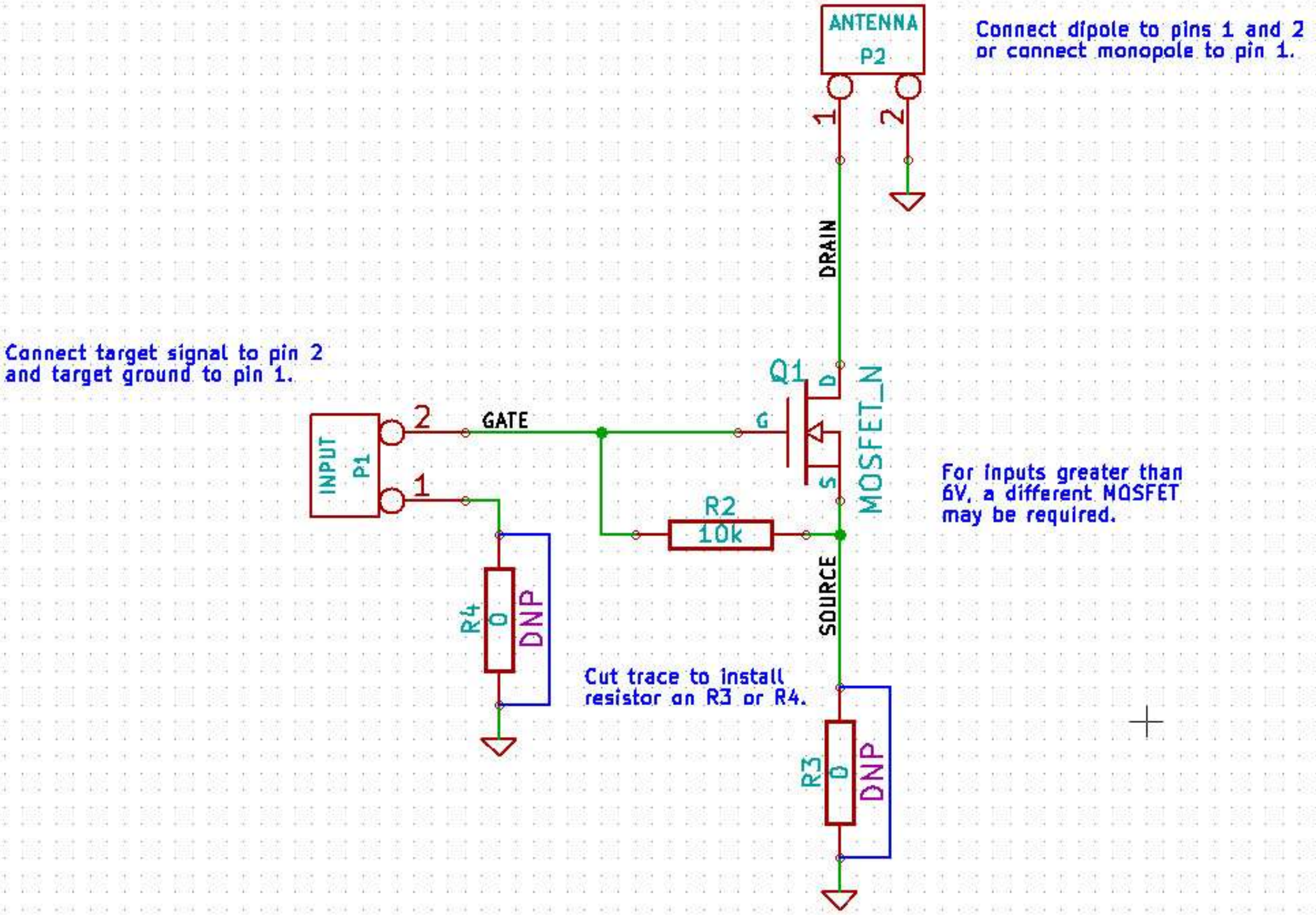
easy to find filters/amplifiers

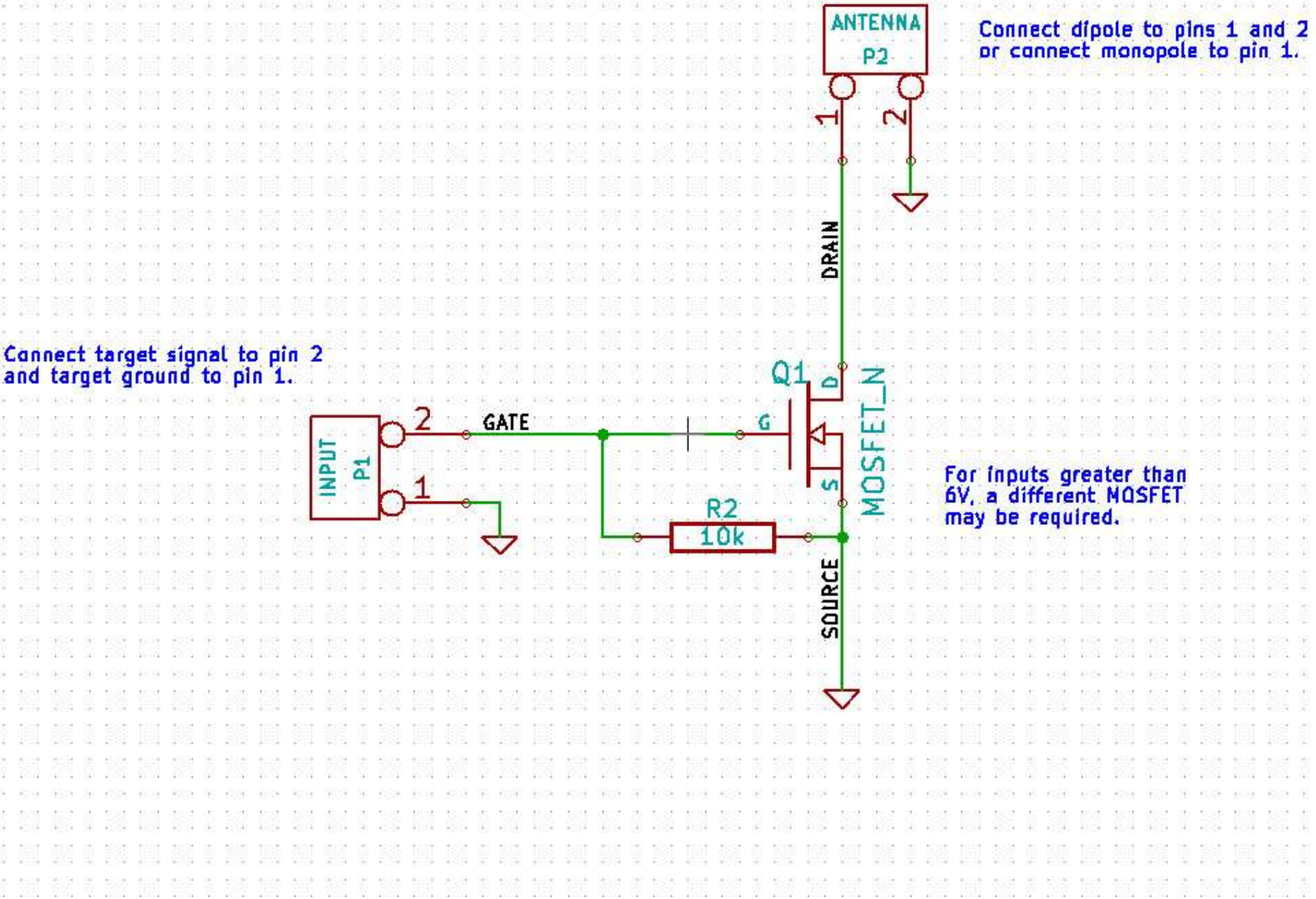
CONGAFLOCK

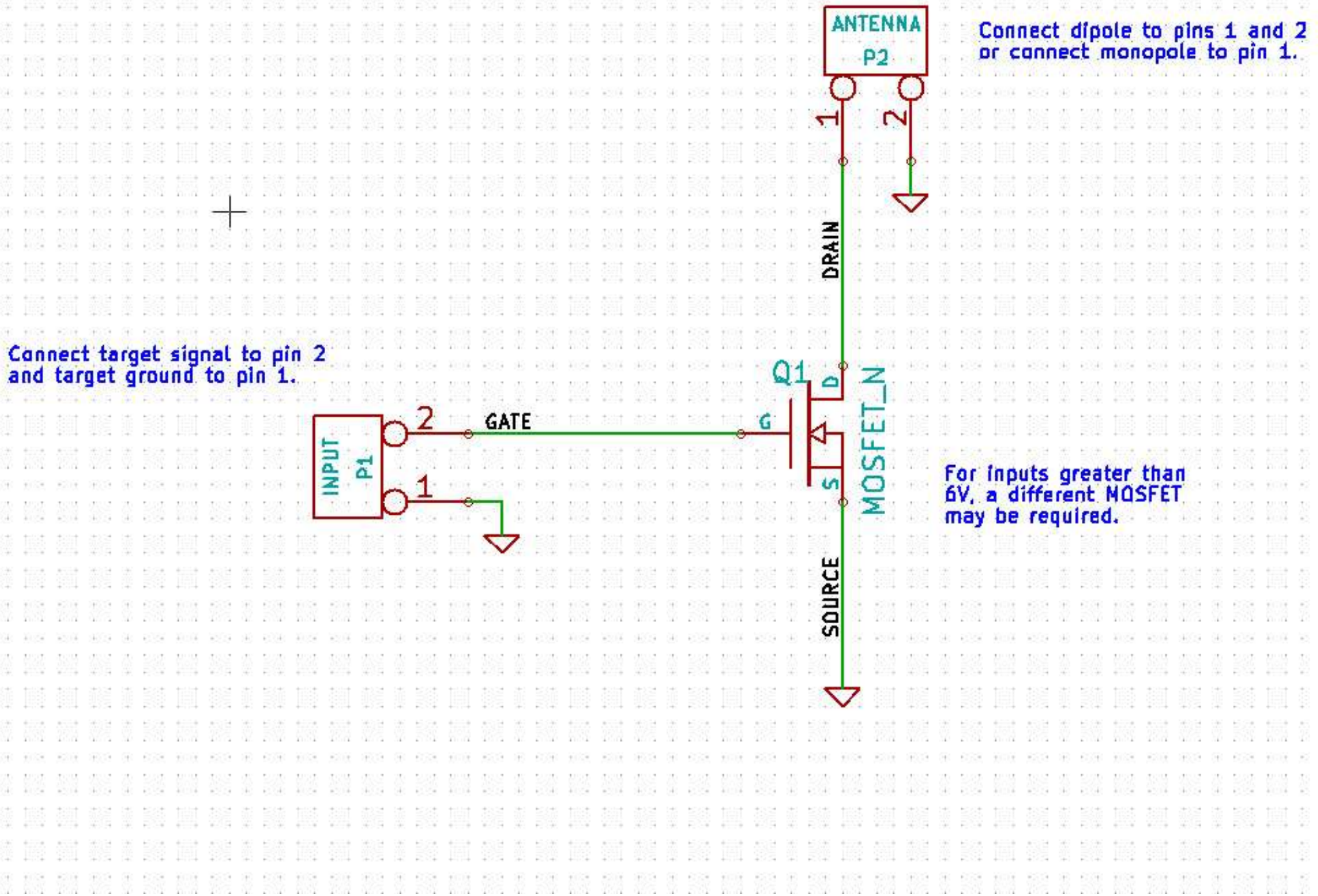


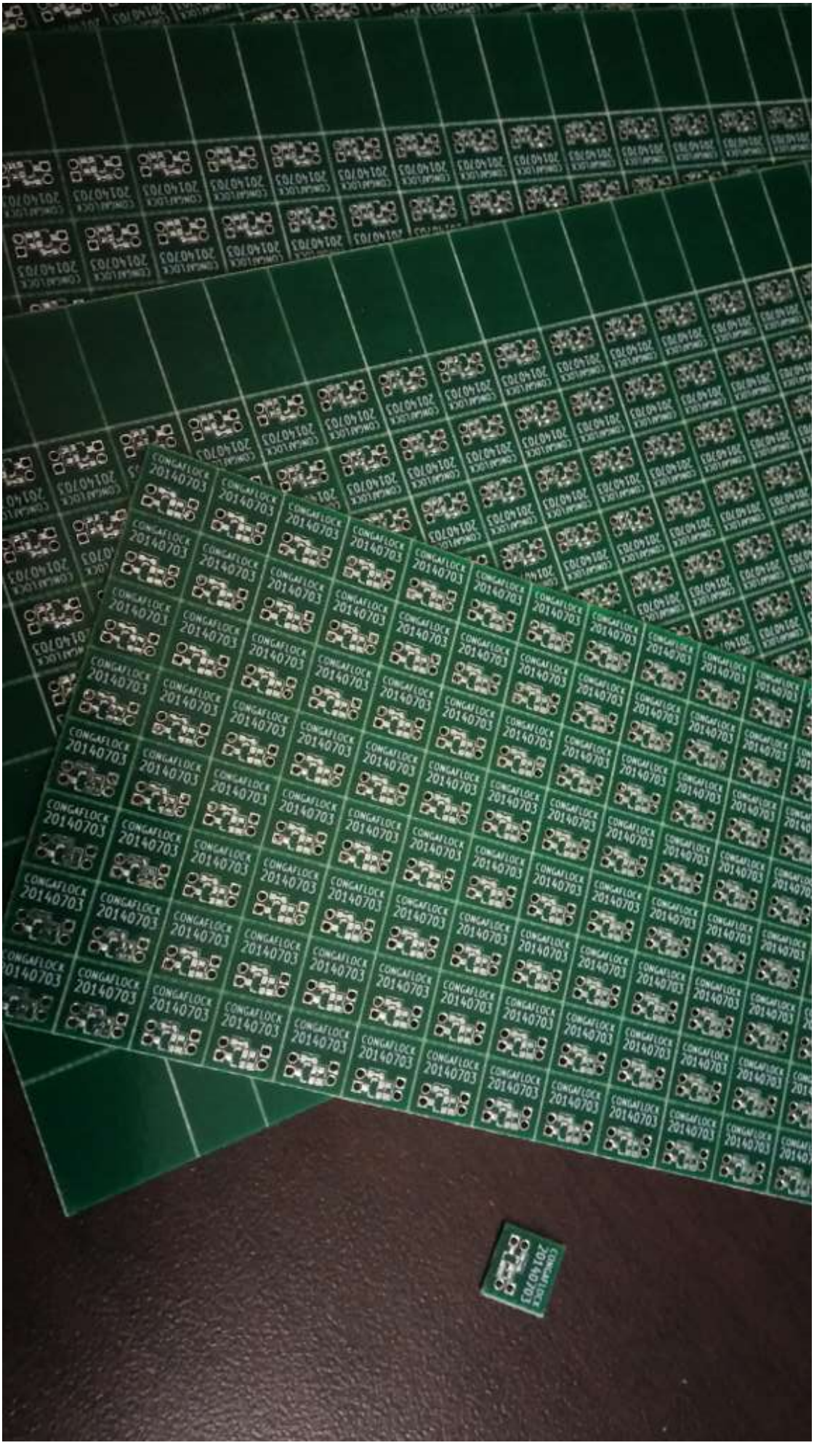

Why
so
large?


ANTENNA
P2
1
2
Connect dipole to pins 1 and 2
or connect monopole to pin 1.
DRAIN
R1
DNP
DNP
Q1
D
G
S
MOSFET_N
Connect target signal to pin 2
and target ground to pin 1.
INPUT
P1
2
1
GATE
R2
10k
For inputs greater than
6V, a different MOSFET
may be required.
R4
0
DNP
Cut trace to install
resistor on R3 or R4.
SOURCE
R3
0
DNP


ANTENNA
P2
1
2
Connect dipole to pins 1 and 2
or connect monopole to pin 1.
DRAIN
Connect target signal to pin 2
and target ground to pin 1.
Q1
D
G
S
MOSFET_N
INPUT
P1
2
GATE
1
R2
10k
For inputs greater than
6V, a different MOSFET
may be required.
R4
0
DNP
SOURCE
Cut trace to install
resistor on R3 or R4.
R3
0
DNP

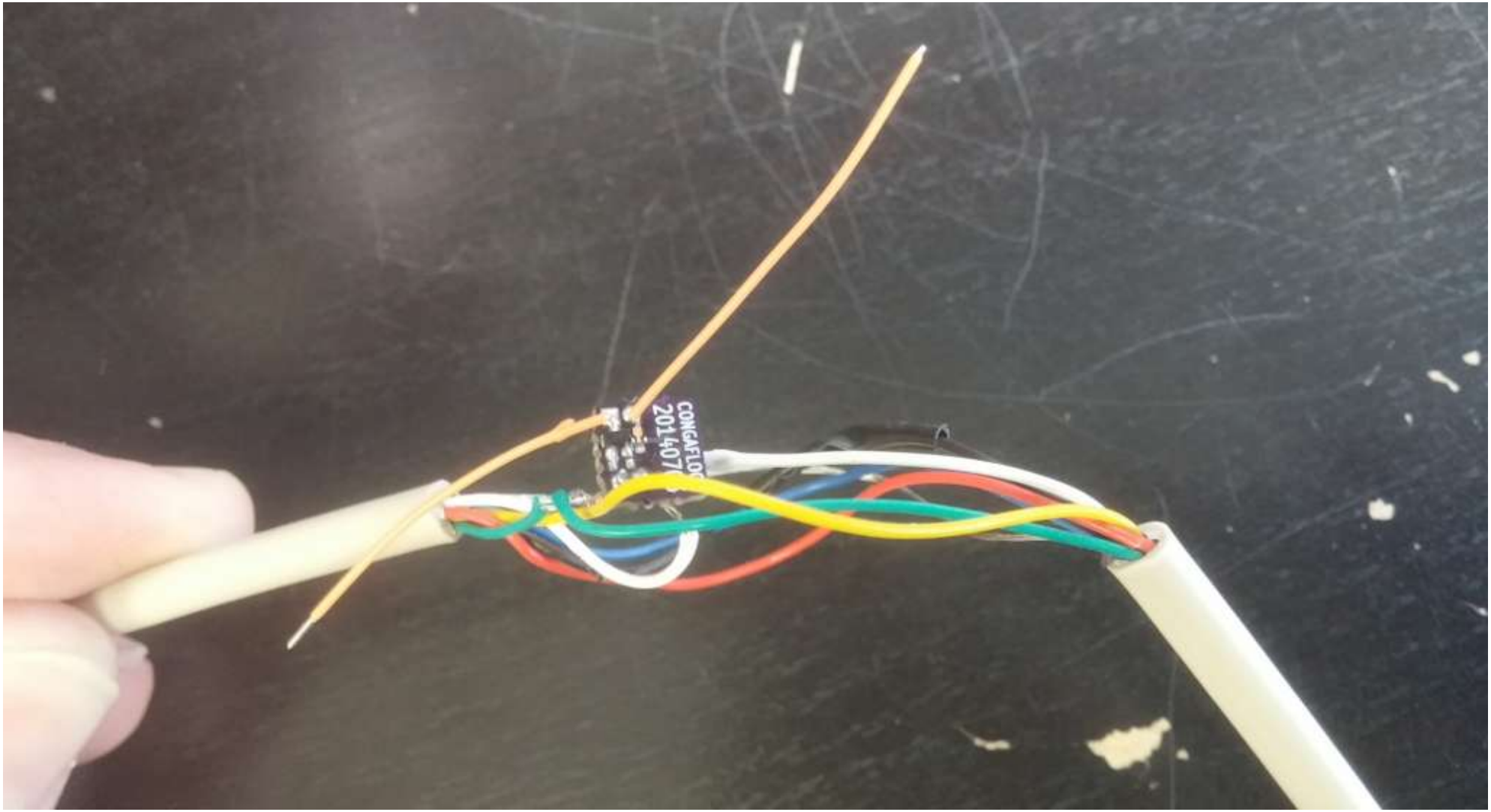

ANTENNA
P2
1
2
Connect dipole to pins 1 and 2
or connect monopole to pin 1.
DRAIN
Connect target signal to pin 2
and target ground to pin 1.
Q1
D
G
S
MOSFET_N
INPUT
P1
2
1
GATE
R2
10k
SOURCE
For inputs greater than
6V, a different MOSFET
may be required.


ANTENNA
P2
1
2
Connect dipole to pins 1 and 2
or connect monopole to pin 1.
DRAIN
Connect target signal to pin 2
and target ground to pin 1.
Q1
D
G
S
MOSFET_N
INPUT
P1
2
GATE
1
For inputs greater than
6V, a different MOSFET
may be required.
SOURCE

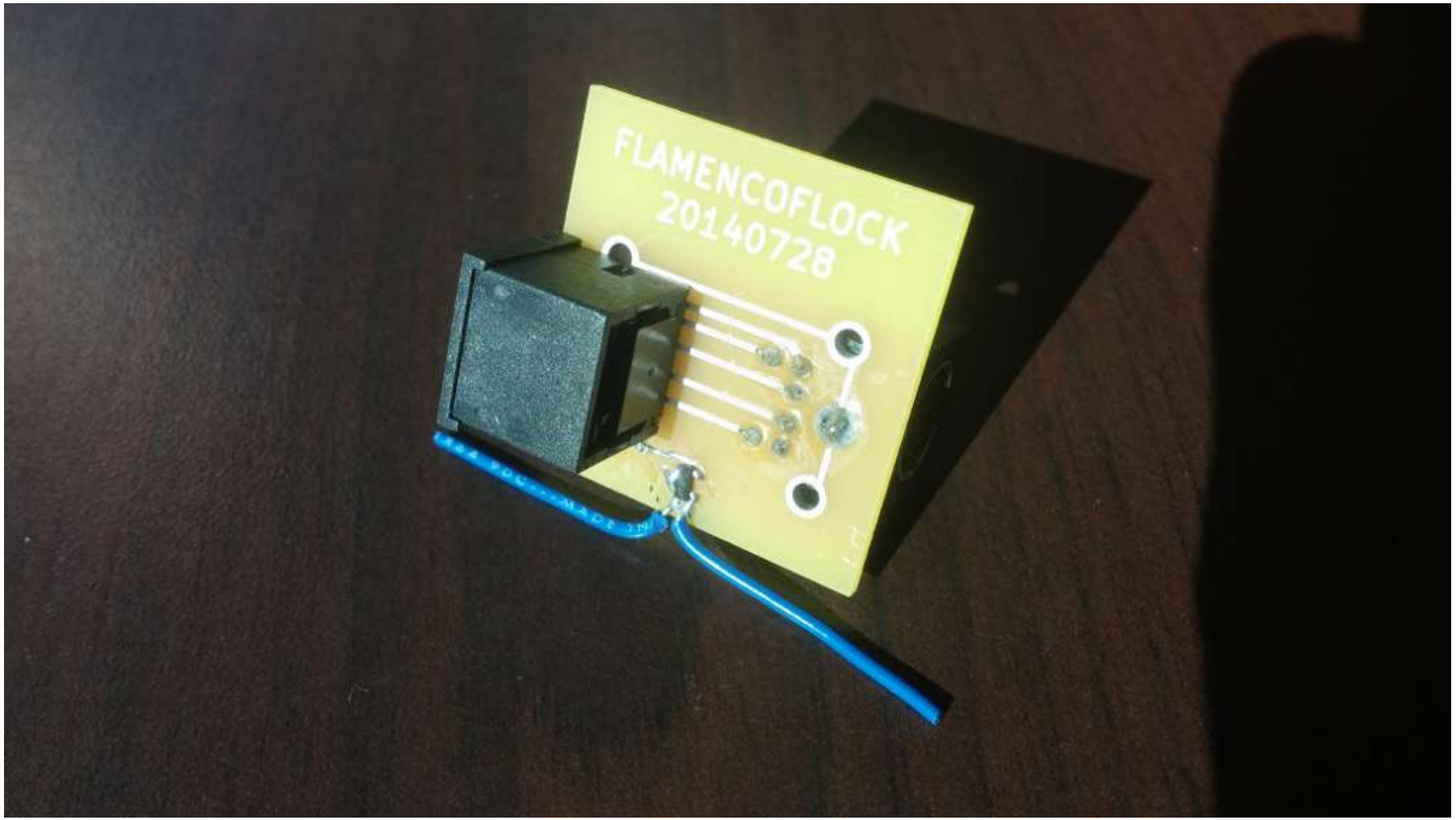

CONGAFLOCK
20140703

Build Your Own

1. Break off PCB
2. Cut two antenna wires (about 1 inch each)
3. Solder MOSFET
4. Solder antenna wires
5. Connect to target

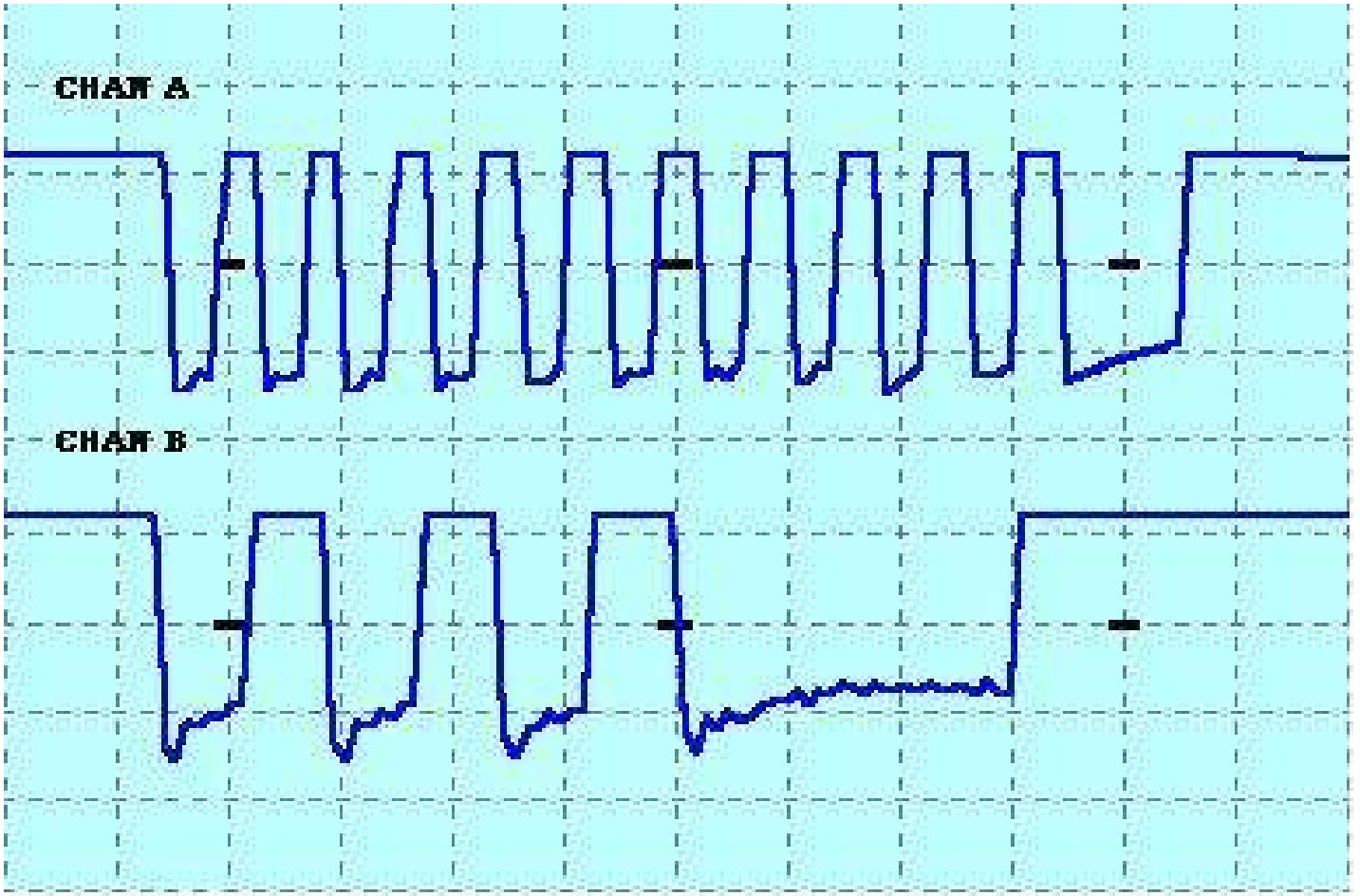


FLAMENCOFLOCK

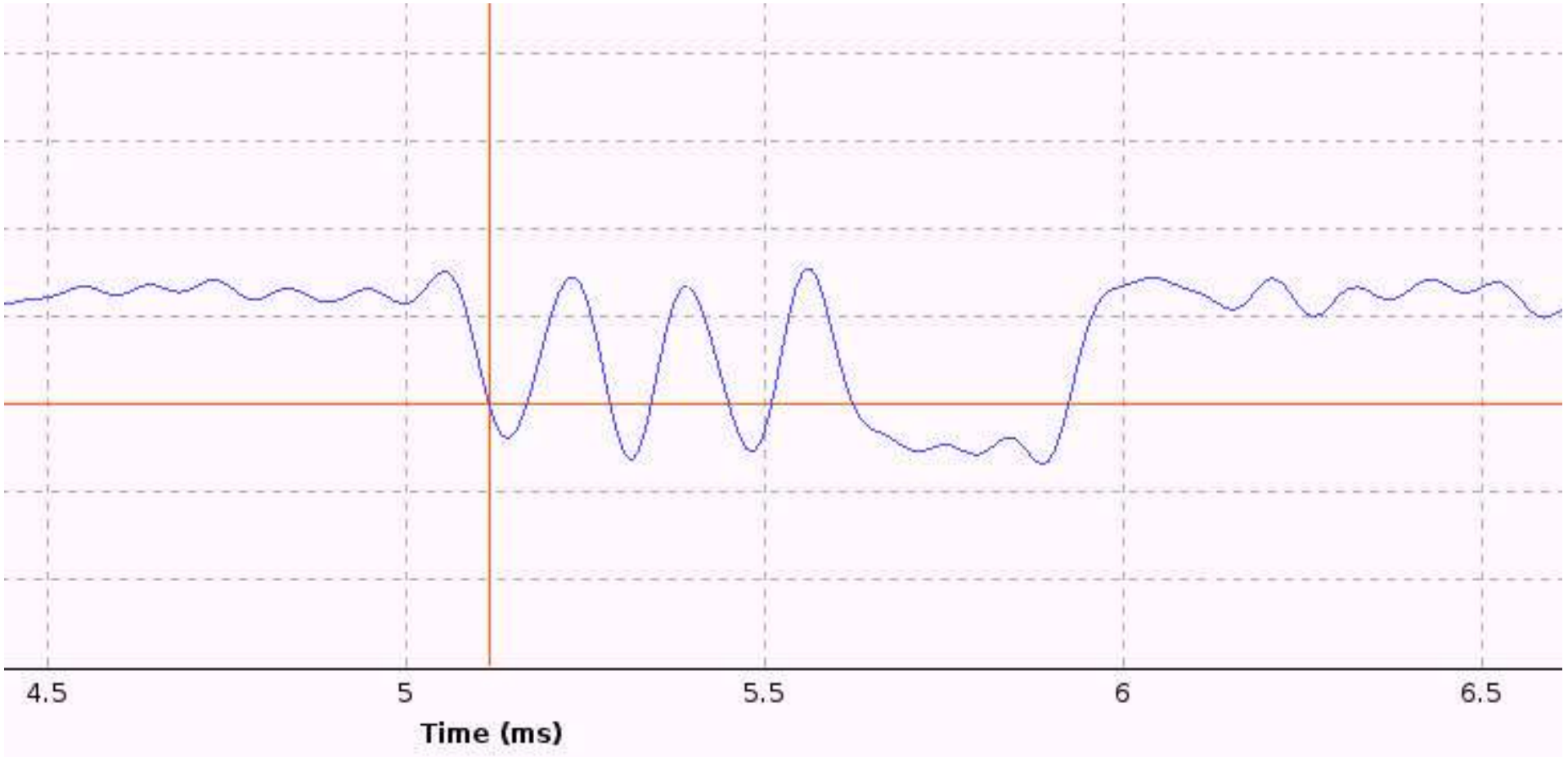


PS/2 keyboard

The Letter Q



http://www.computer-engineering.org/ps2protocol/


4.5
5
5.5
6
6.5
Time (ms)

TANGOFLOCK

USB

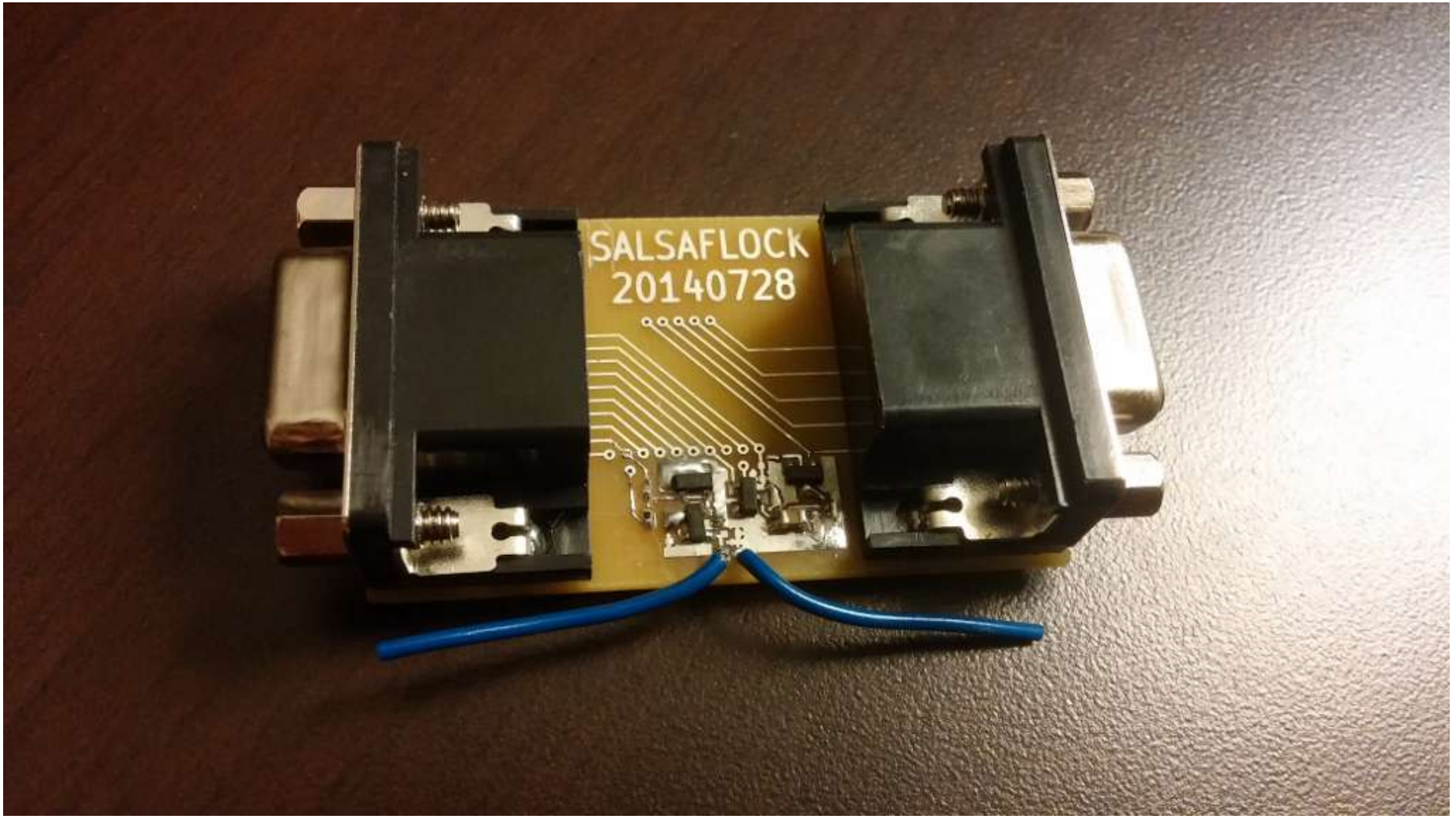
Low Speed USB: briefly tested

Full Speed USB: likely works

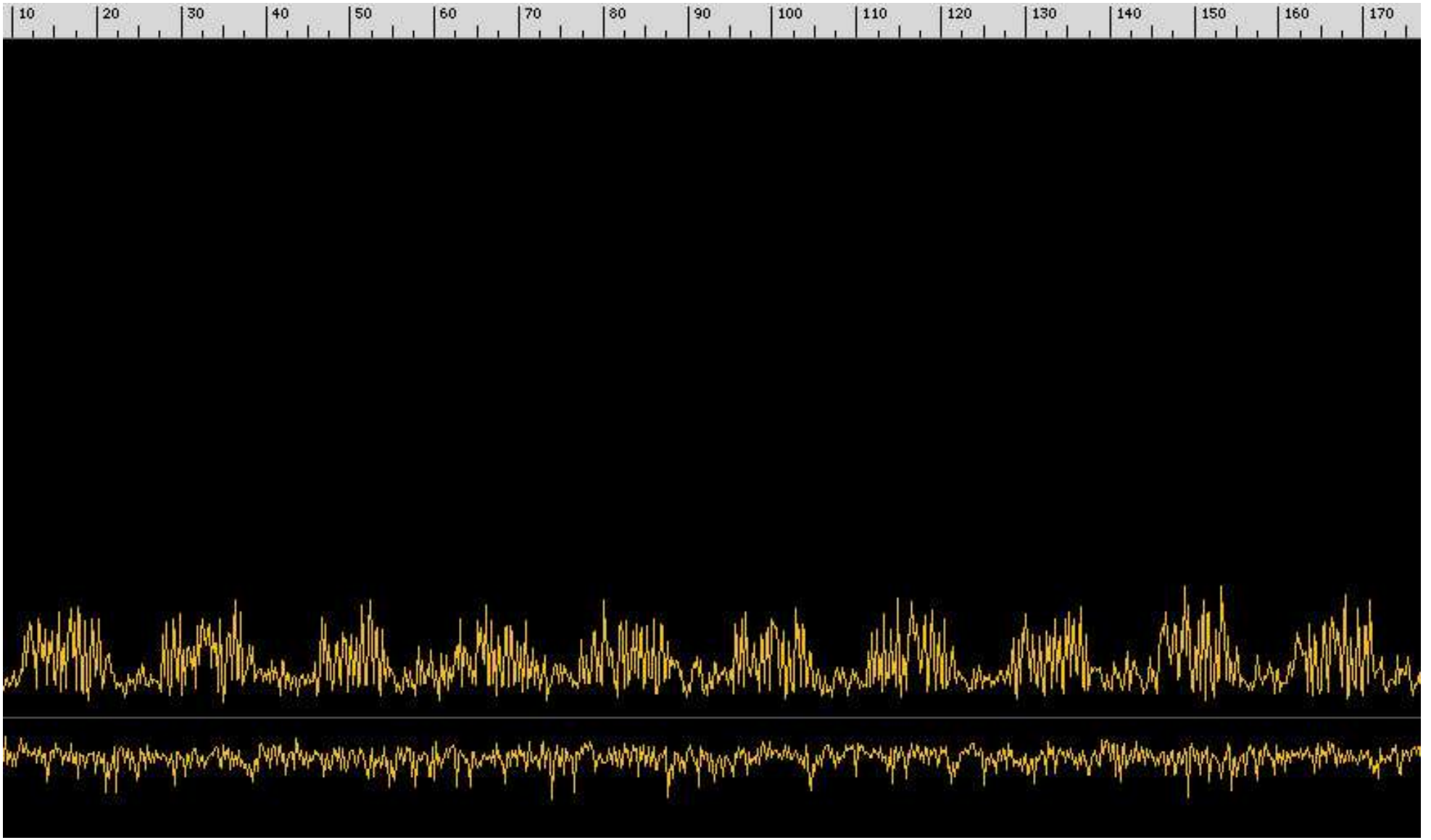
Hi-Speed USB: probably not (need lots of bandwidth)

SuperSpeed USB: definitely not (no connection)

SALSAFLOCK



VGA

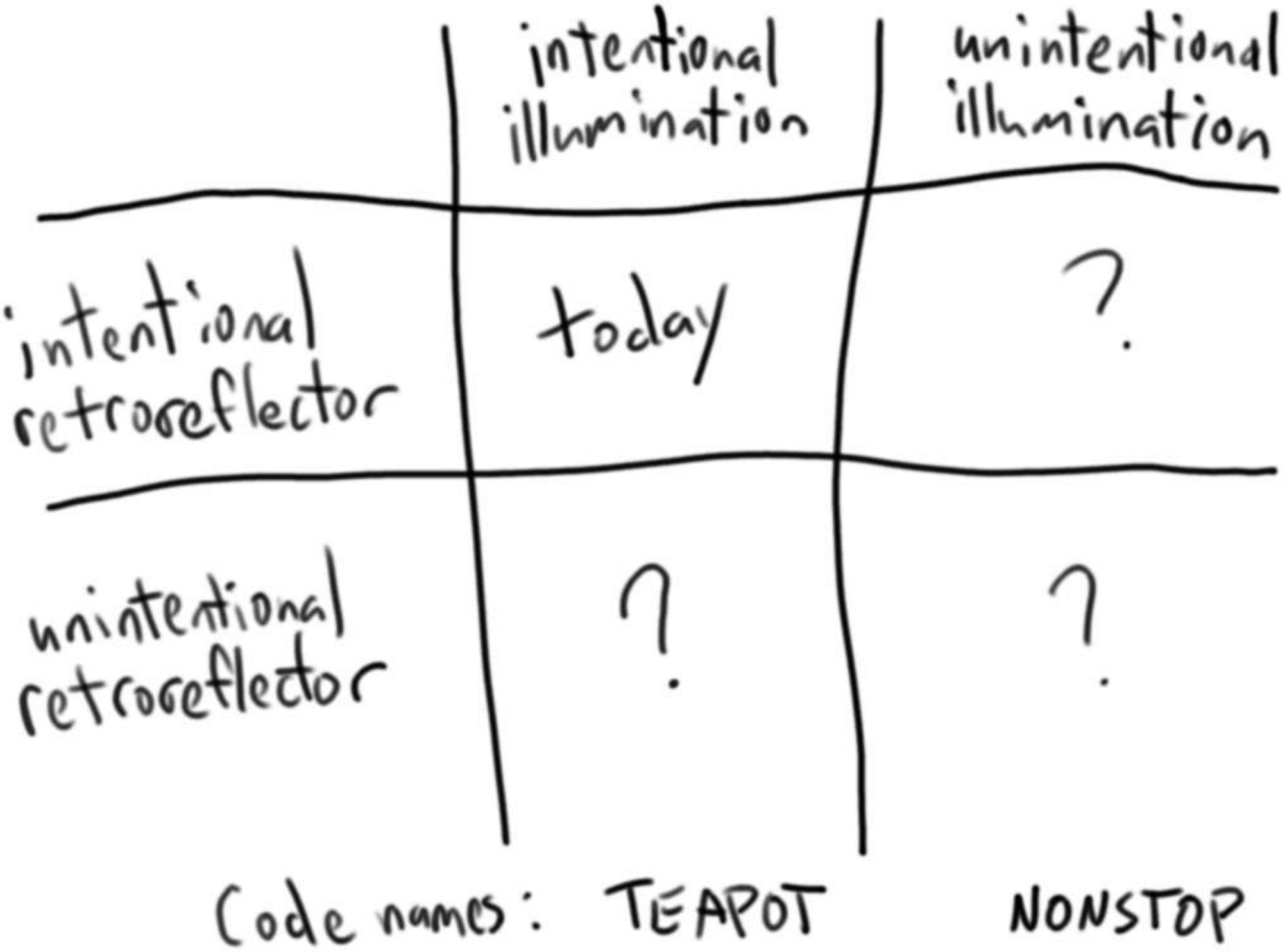

10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170

Countermeasures

Invitation to Hack

much more research
to be done

SDR is a great tool
(video series coming soon!)


intentional illumination
unintentional illumination
intentional retroreflector
today
?
unintentional retroreflector
?
?
Code names: TEAPOT NONSTOP

Be a Good Neighbor

know your laws

don't interfere

Thank You

Dean Pierce and the whole NSA Playset crew
Nick Malar (illustrations)
Jared Boone

nsaplayset.org

github.com/mossmann/retroreflectors

greatscottgadgets.com