

# RF Retroreflectors, Emission Security, and SDR

Michael Ossmann  
Great Scott Gadgets

no  
leaked  
classified  
content

# The NSA Playset

Play along with the NSA!

Ossmann & Pierce, ToorCamp 2014:

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



NSA Playset

HackRF One

PLAST

# RF Retroreflectors

Attacker

Target



# The State of Emission Security

unintentional  
emissions

vs.

reflective RF  
attacks



# The Thing



(Great Seal Bug)

# A History of Reflective RF Attacks

1960  
The Thing

2013  
ANT catalog



53 years of  
rumor and speculation



# RF Backscatter Communication

well researched

# Communication by Means of Reflected Power

Harry Stockman, 1948

lots of more  
recent research

especially UHF RFID

	intentional illumination	unintentional illumination
intentional retroreflector	today	?
unintentional retroreflector	?	?

Code names: TEAPOT

NONSTOP

# 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







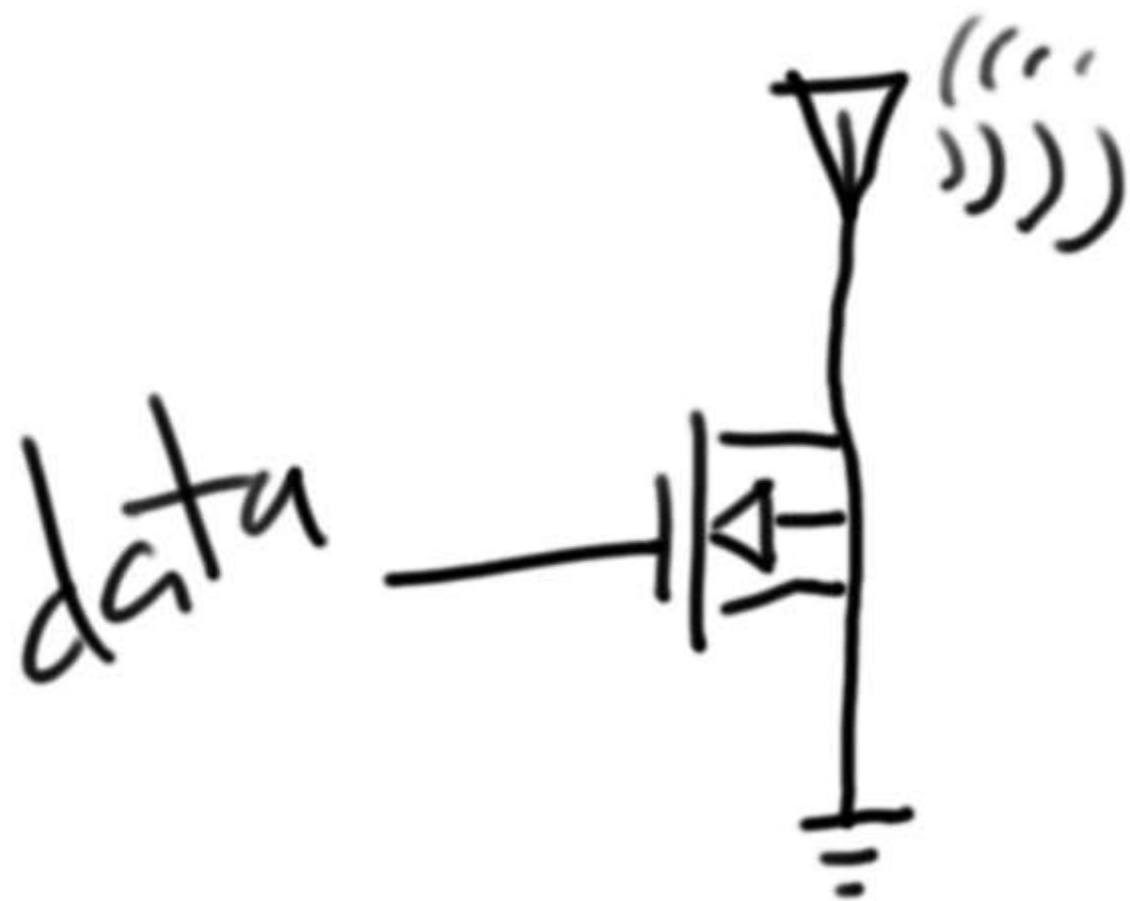
GREAT SCOTT GADGETS  
**HACKRF One**  
GREAT SCOTT GADGETS

**HackRF One**  
GREAT SCOTT GADGETS

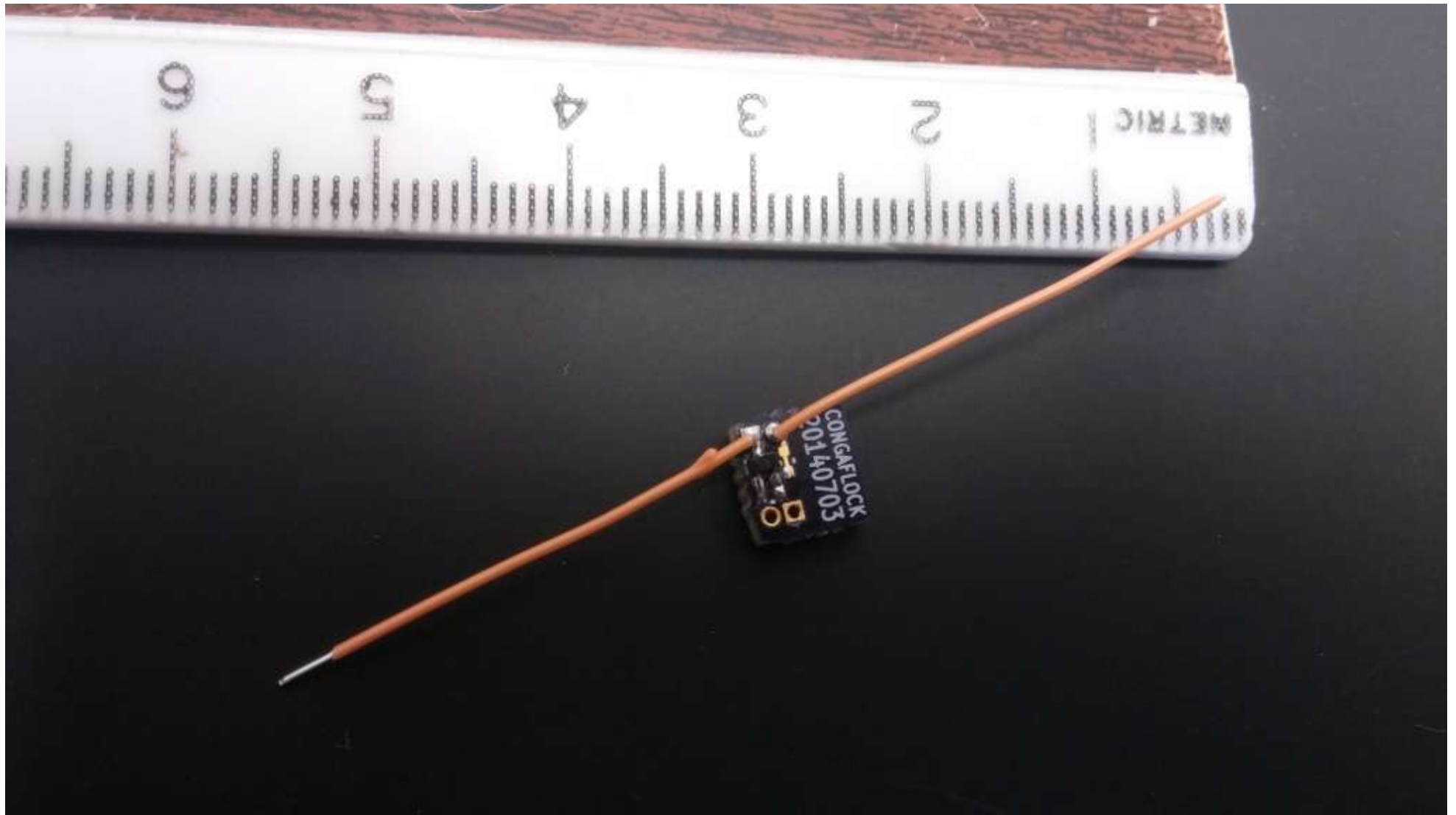
**HackRF One**  
GREAT SCOTT GADGETS



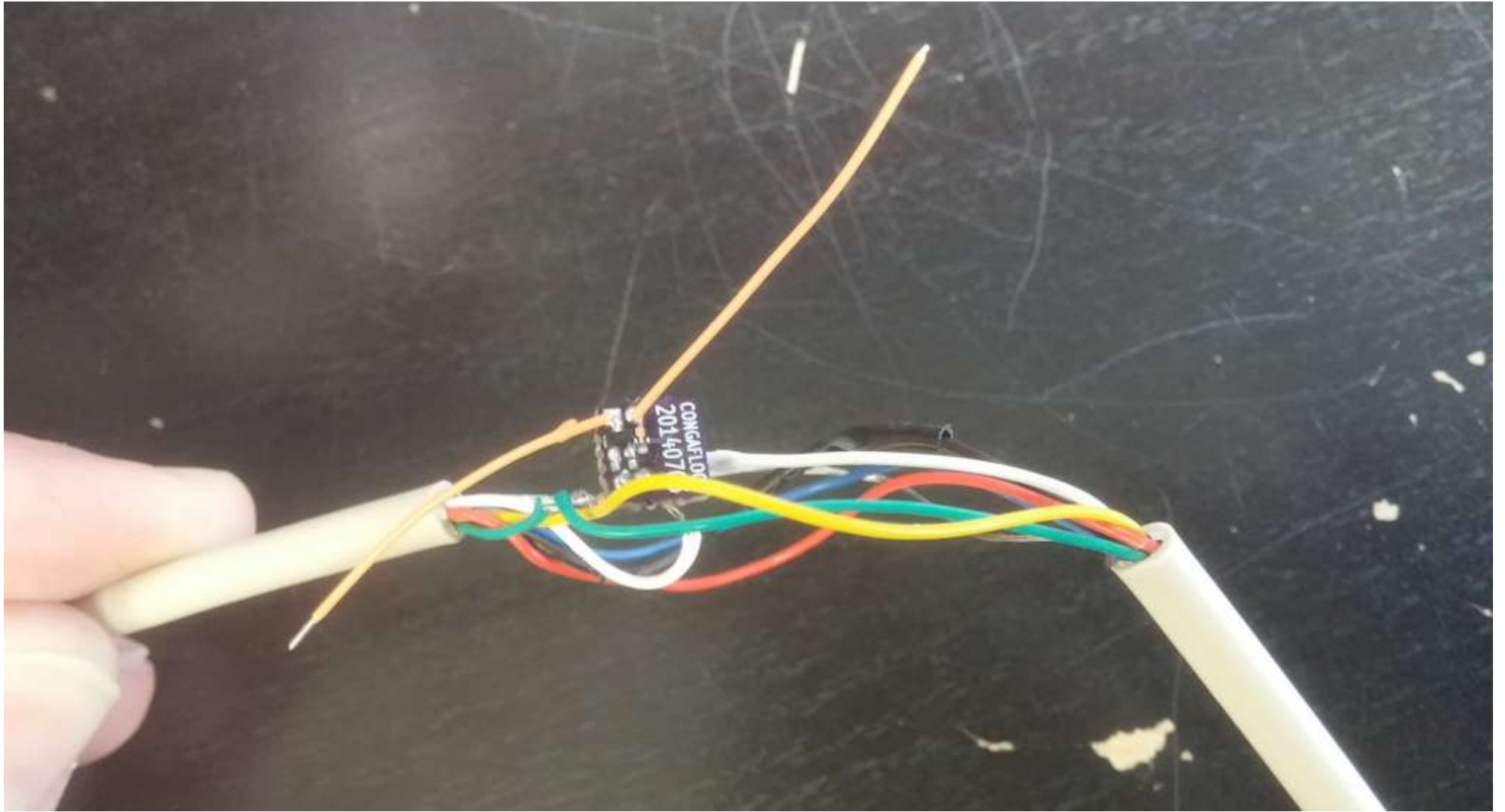
# Simple RF Retroreflector



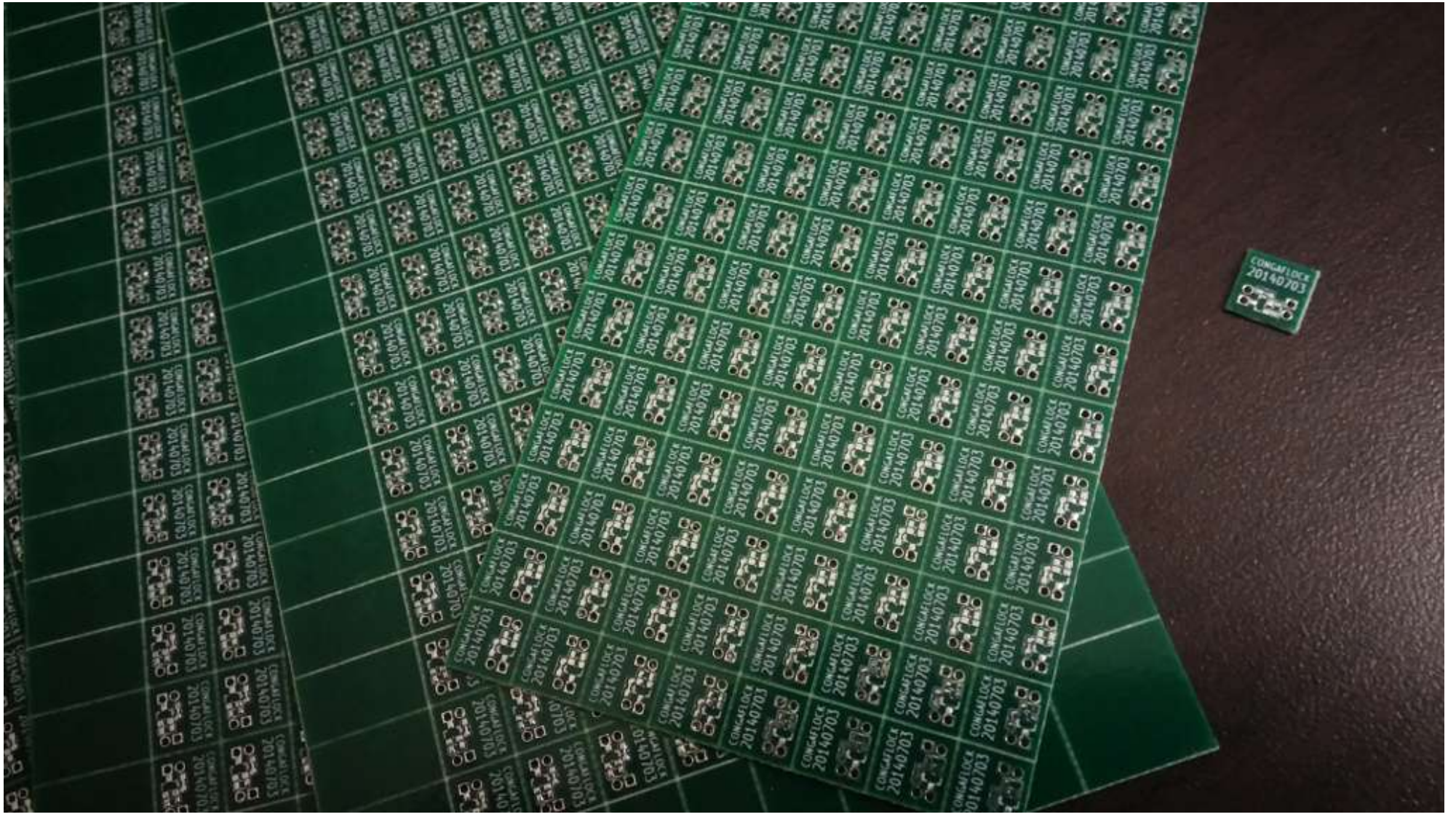
# CONGAFLOCK









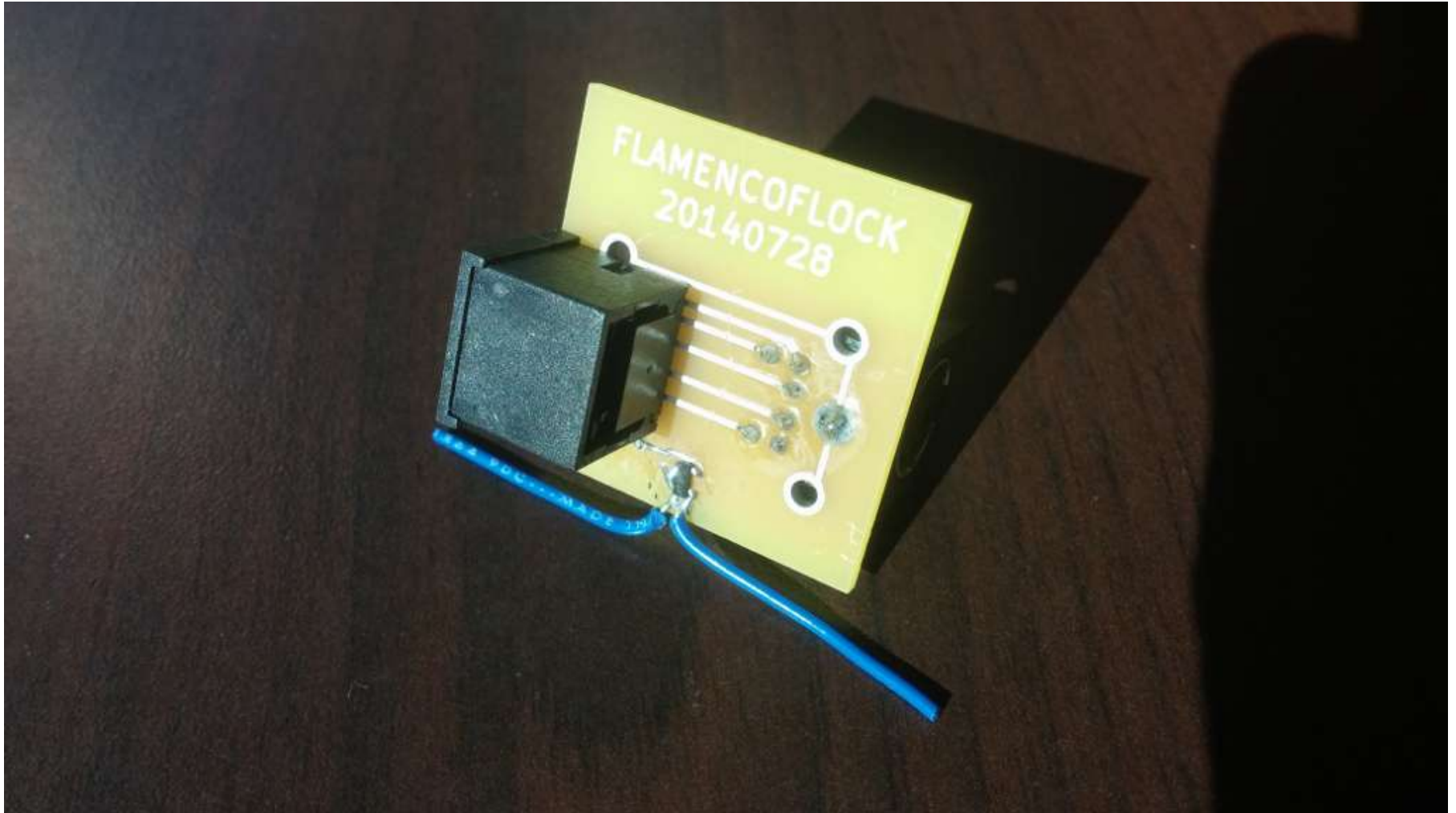




# Build Your Own

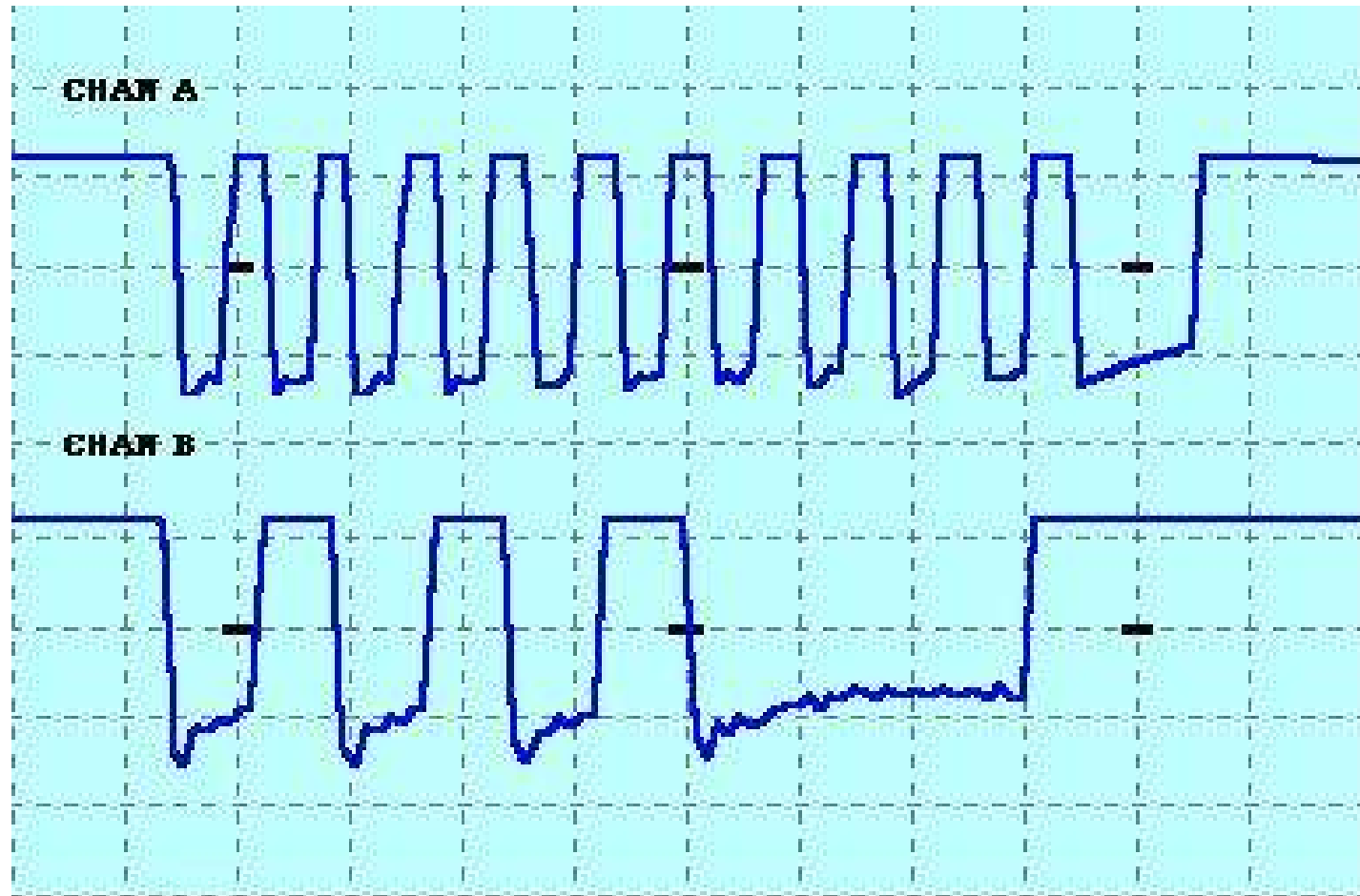


# FLAMENCOFLOCK

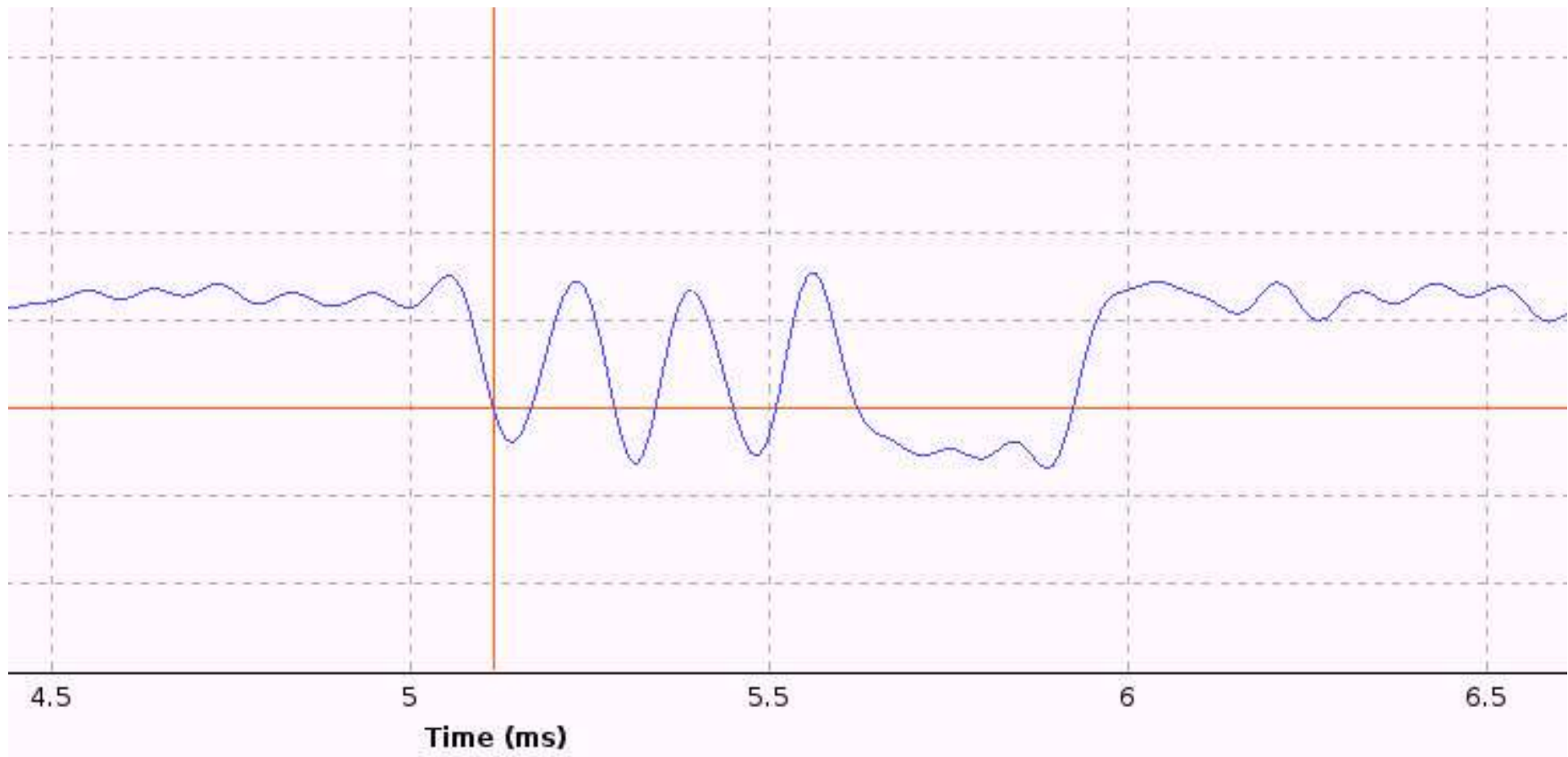


PS/2 keyboard

# The Letter Q



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





# TANGOFLOCK



USB



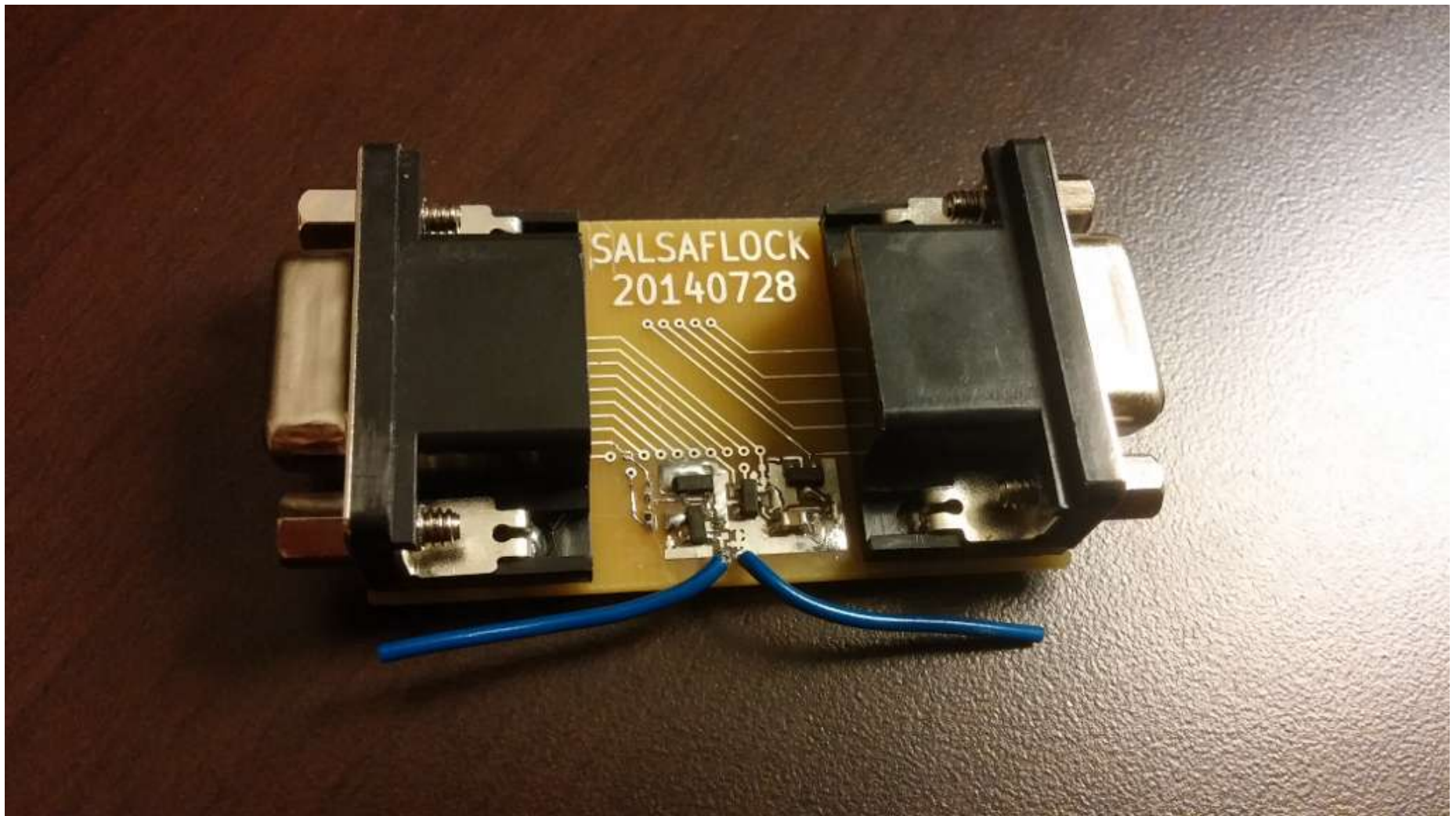
Low Speed USB: briefly  
tested

Full Speed USB: likely works

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

SuperSpeed USB: definitely not  
(no connection)

SALSAFLOCK



VGA

root@pentoo:~#

ss -ltn

root@pentoo:~#

```

1024x768      75.1      60.0
800x600       75.0      60.3
640x480       75.0      60.0*
720x400       70.1

```

DPI disconnected (normal left inverted right x axis y axis)

TVI unknown connection (normal left inverted right x axis y axis)

```

848x480      59.9 +
640x480      59.9 +
1024x768     59.9
800x600      59.9

```

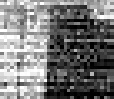
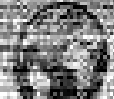
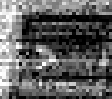
pentoo #

pentoo #

pentoo #

pentoo #

pentoo #





10/1	Balance	1000.00	
10/2	Income		500.00
10/3	Expenses	200.00	
10/4	Income		300.00
10/5	Expenses	150.00	
10/6	Income		400.00
10/7	Expenses	100.00	
10/8	Income		250.00
10/9	Expenses	80.00	
10/10	Income		350.00
10/11	Expenses	60.00	
10/12	Income		450.00
10/13	Expenses	40.00	
10/14	Income		550.00
10/15	Expenses	20.00	
10/16	Income		650.00
10/17	Expenses	10.00	
10/18	Income		750.00
10/19	Expenses	5.00	
10/20	Income		850.00
10/21	Expenses	2.50	
10/22	Income		950.00
10/23	Expenses	1.25	
10/24	Income		1050.00
10/25	Expenses	0.625	
10/26	Income		1150.00
10/27	Expenses	0.3125	
10/28	Income		1250.00
10/29	Expenses	0.15625	
10/30	Income		1350.00
10/31	Expenses	0.078125	
Total		1350.00	1350.00

10/31 Balance forward 1350.00  
 11/1 Balance forward 1350.00

11/1	Income		100.00
11/2	Expenses	50.00	
11/3	Income		150.00
11/4	Expenses	75.00	
11/5	Income		200.00
11/6	Expenses	100.00	
11/7	Income		250.00
11/8	Expenses	125.00	
11/9	Income		300.00
11/10	Expenses	150.00	
11/11	Income		350.00
11/12	Expenses	175.00	
11/13	Income		400.00
11/14	Expenses	200.00	
11/15	Income		450.00
11/16	Expenses	225.00	
11/17	Income		500.00
11/18	Expenses	250.00	
11/19	Income		550.00
11/20	Expenses	275.00	
11/21	Income		600.00
11/22	Expenses	300.00	
11/23	Income		650.00
11/24	Expenses	325.00	
11/25	Income		700.00
11/26	Expenses	350.00	
11/27	Income		750.00
11/28	Expenses	375.00	
11/29	Income		800.00
11/30	Expenses	400.00	
Total		800.00	800.00

- 11/31 Balance forward 800.00
- 12/1 Balance forward 800.00
- 12/2 Balance forward 800.00
- 12/3 Balance forward 800.00
- 12/4 Balance forward 800.00
- 12/5 Balance forward 800.00
- 12/6 Balance forward 800.00
- 12/7 Balance forward 800.00
- 12/8 Balance forward 800.00
- 12/9 Balance forward 800.00
- 12/10 Balance forward 800.00
- 12/11 Balance forward 800.00
- 12/12 Balance forward 800.00
- 12/13 Balance forward 800.00
- 12/14 Balance forward 800.00
- 12/15 Balance forward 800.00
- 12/16 Balance forward 800.00
- 12/17 Balance forward 800.00
- 12/18 Balance forward 800.00
- 12/19 Balance forward 800.00
- 12/20 Balance forward 800.00
- 12/21 Balance forward 800.00
- 12/22 Balance forward 800.00
- 12/23 Balance forward 800.00
- 12/24 Balance forward 800.00
- 12/25 Balance forward 800.00
- 12/26 Balance forward 800.00
- 12/27 Balance forward 800.00
- 12/28 Balance forward 800.00
- 12/29 Balance forward 800.00
- 12/30 Balance forward 800.00
- 12/31 Balance forward 800.00

11/31 Balance forward 1350.00  
 12/1 Balance forward 1350.00

nsaplayset.org

github.com/mossmann/retroreflectors

greatscottgadgets.com