August 19, 2016


PITCHFORK!!S!

# threat models

# simple model

- mitigated threat
- introduced threat

# pgp threat model

- passive adversary

. . . but we have an active one

# real threat model

adversaries can (amongst others):

- control the victims environment (network, computer, etc.)
- archives cryptograms
- physical access (theft, confiscation, evil maid attacks, etc.)
- interdiction attacks

# traditional mitigations

- use a smartcard against key recovery from general computing device
- use symmetric crypto with one-time-keys instead of pubkey crypto
- offline keys

PITCHFORK (TOP SECRET UMBRA//COMSEC//EYES ONLY//20380119)

- (U//FOUO) PITCHFORK is a device for compartmentalizing key material and cryptographic operations in a small and durable USB device.

# history

- started in 2013
- last year the boards design stabilized
- lots of developments on the firmware

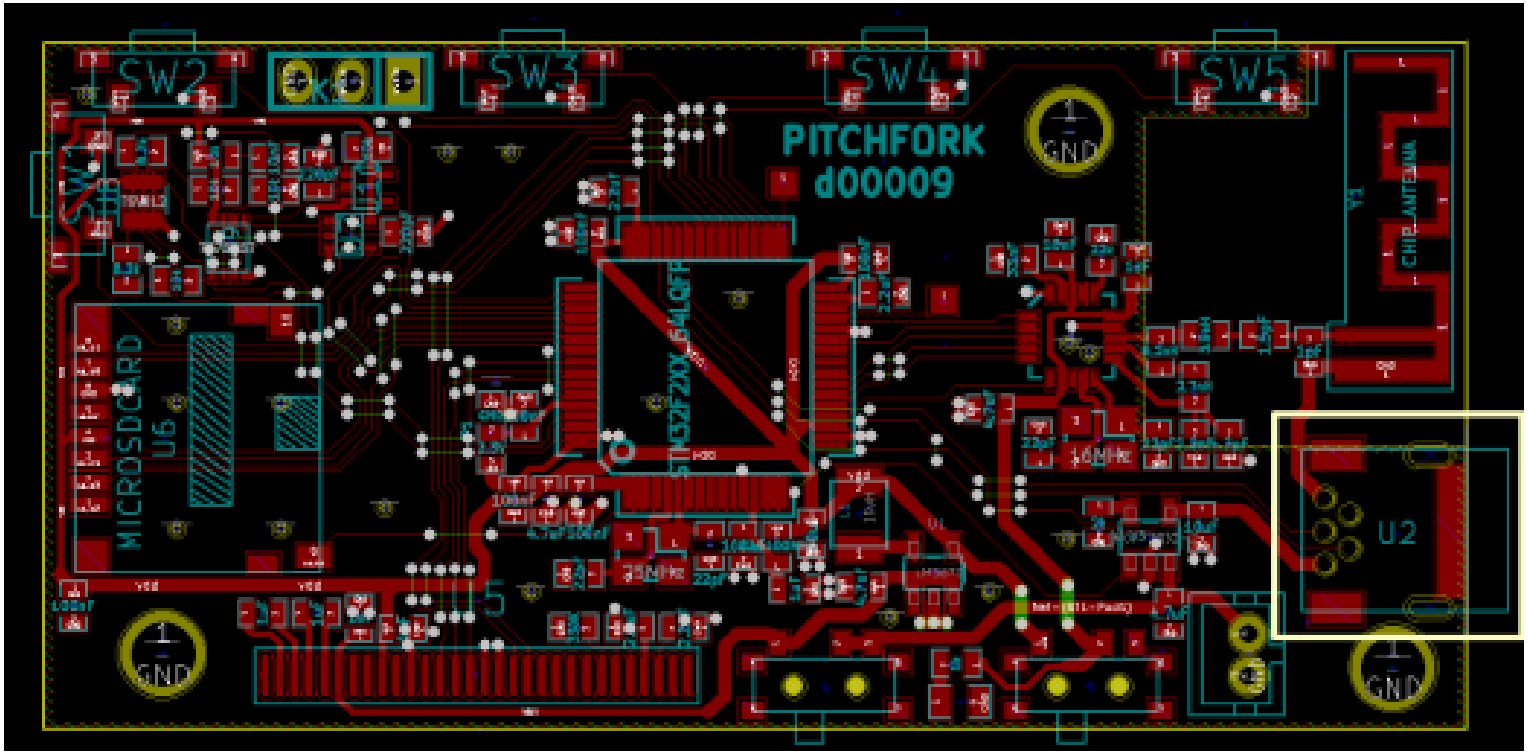

UNDER
CONSTRUCTION

# pitchfork mitigations

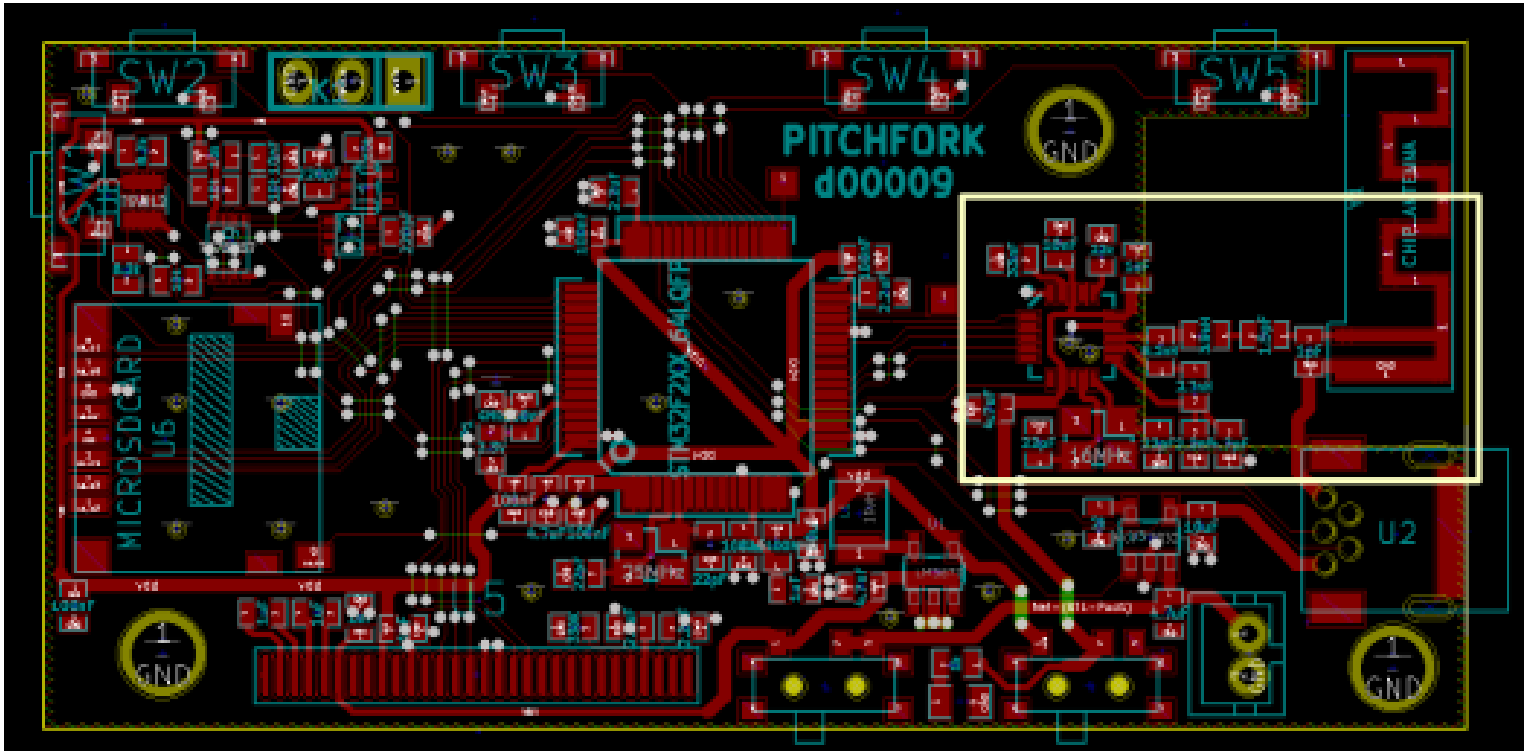
- key recovery from a general purpose computing device
- traffic analysis based on metadata in cryptograms
- attacks from host device via usb
- key compromise during short-term non-intrusive physical access by the adversary (e.g. airports, security checks, etc)
- backdooring during production and shipment
- post-quantum attacks on cryptographic algorithms

peripherials

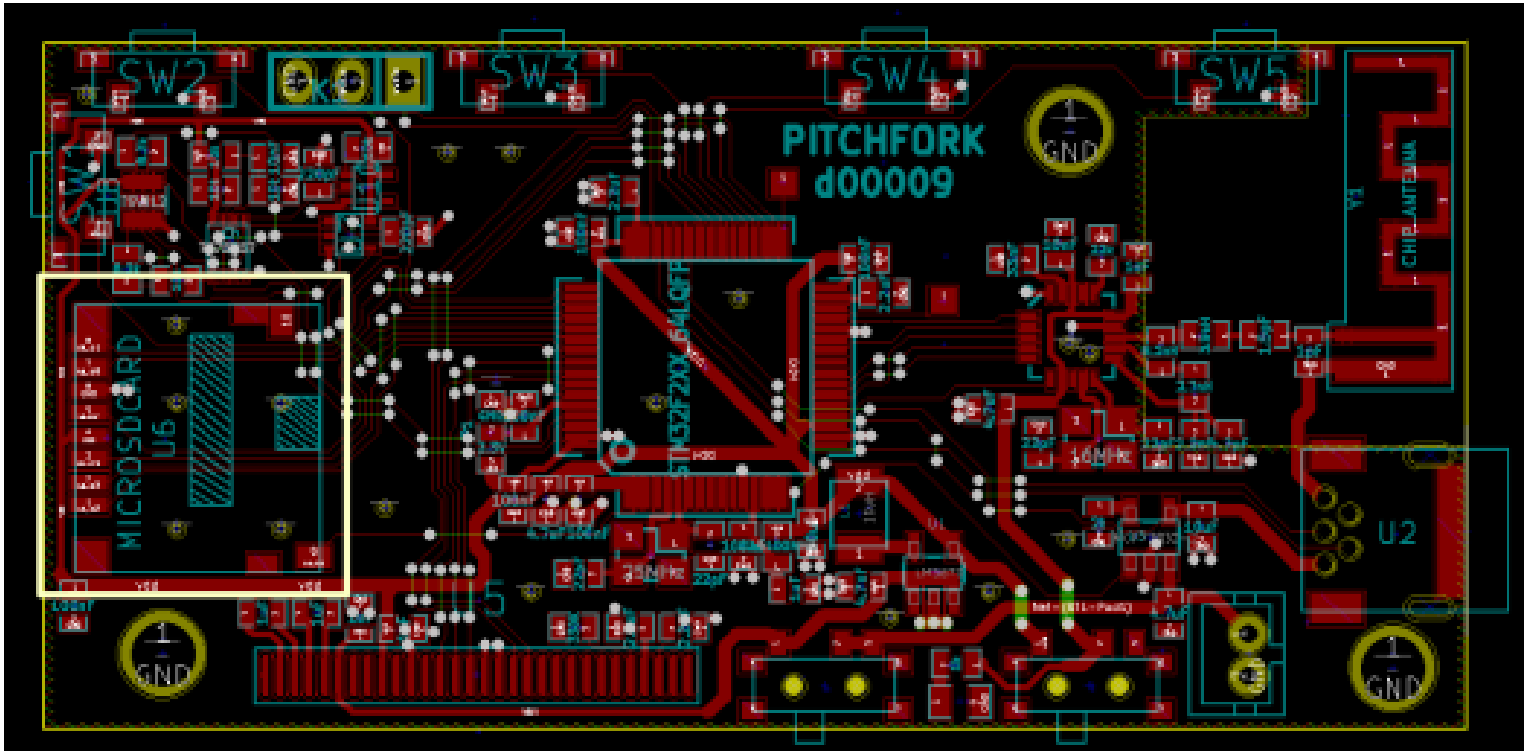
# mini usb


SW2
SW3
SW4
SW5
PITCHFORK
d00009
GND
MICROSDCARD
U5
U2
GND
GND

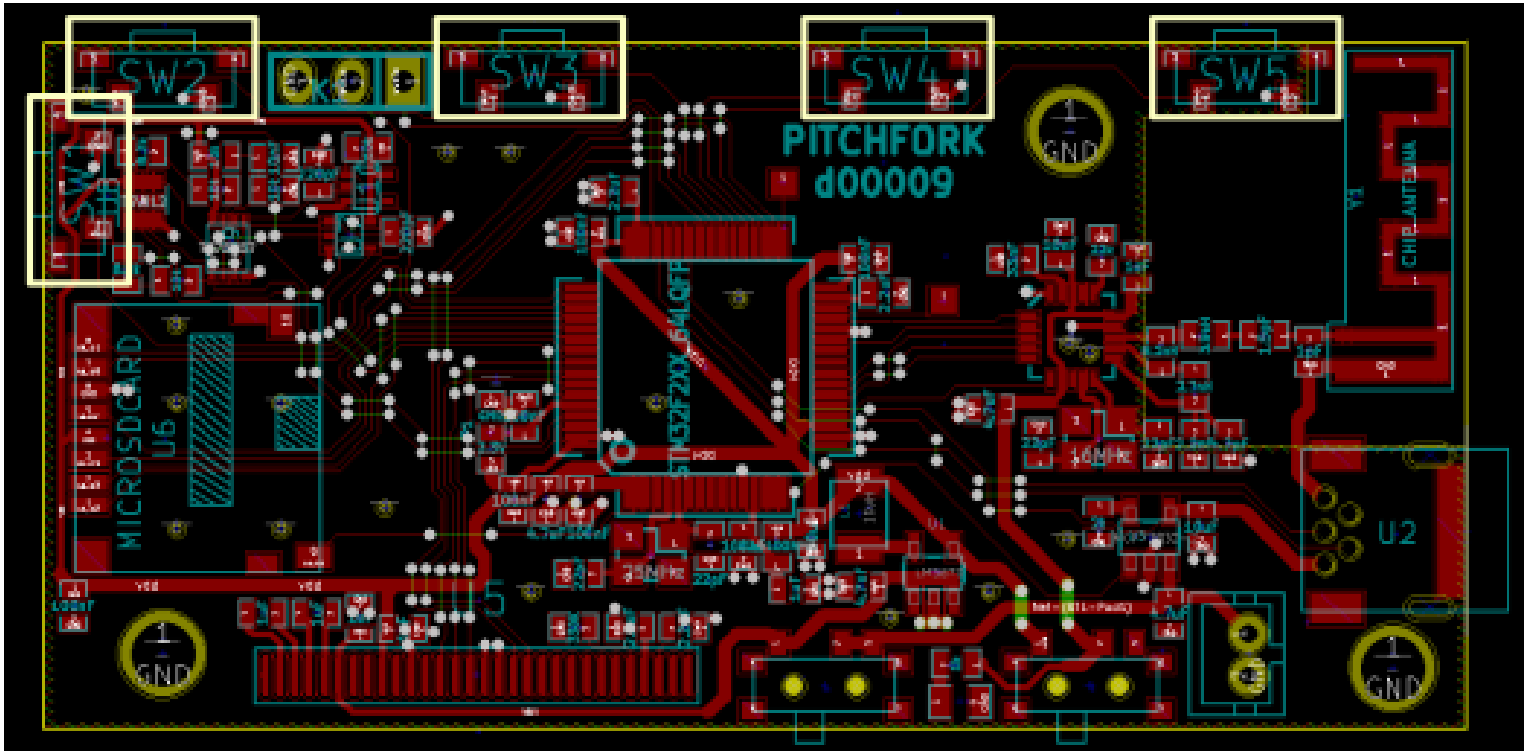
# nrf24l01+


SW2
SW3
SW4
SW5
PITCHFORK
d00009
GND
MICROSDCARD
U5
U2
16MHz
CHIPANTENNA

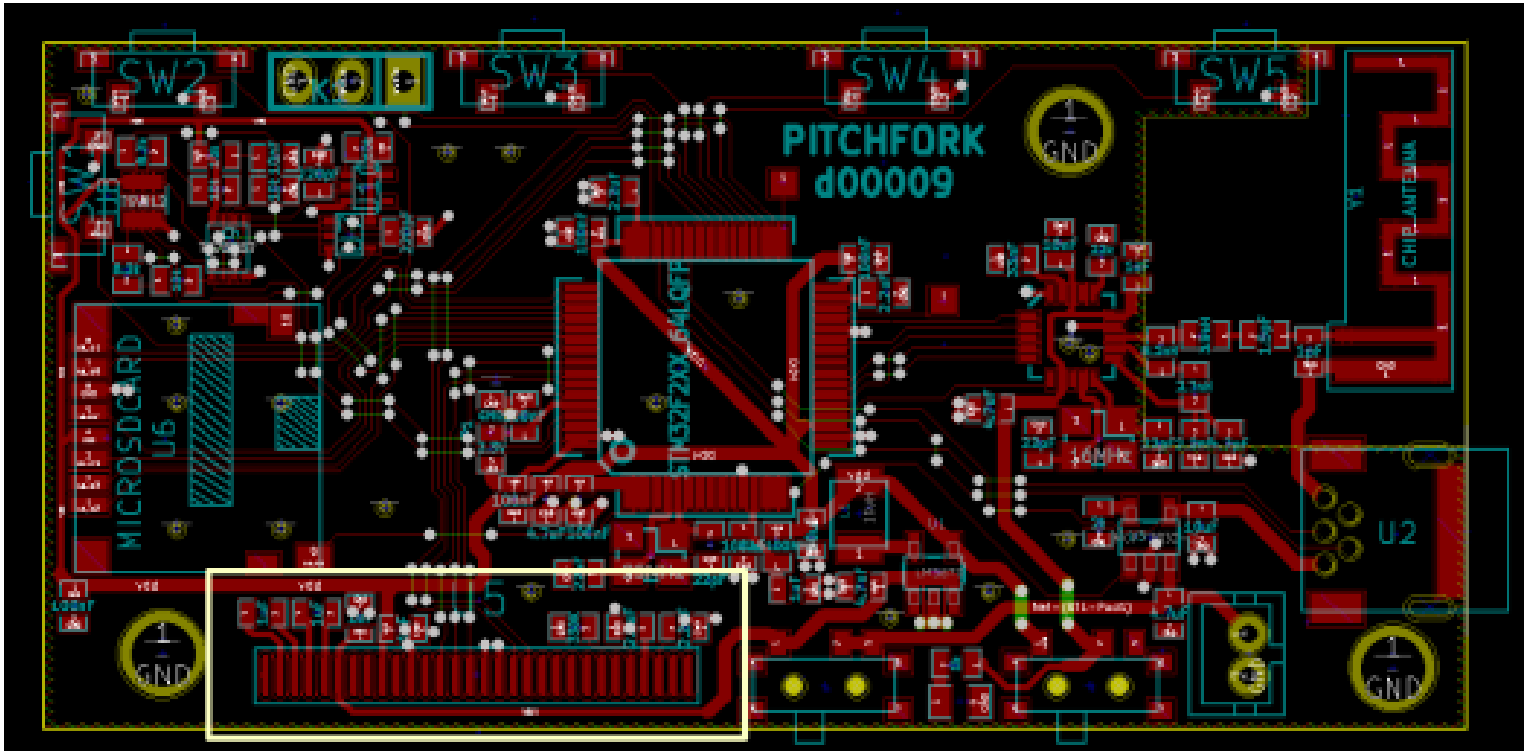
# microsd


SW2
SW3
SW4
SW5
PITCHFORK
d00009
GND
MICROSDCARD
U5
U2
16MHz
32.768kHz
CHIPANTENNA

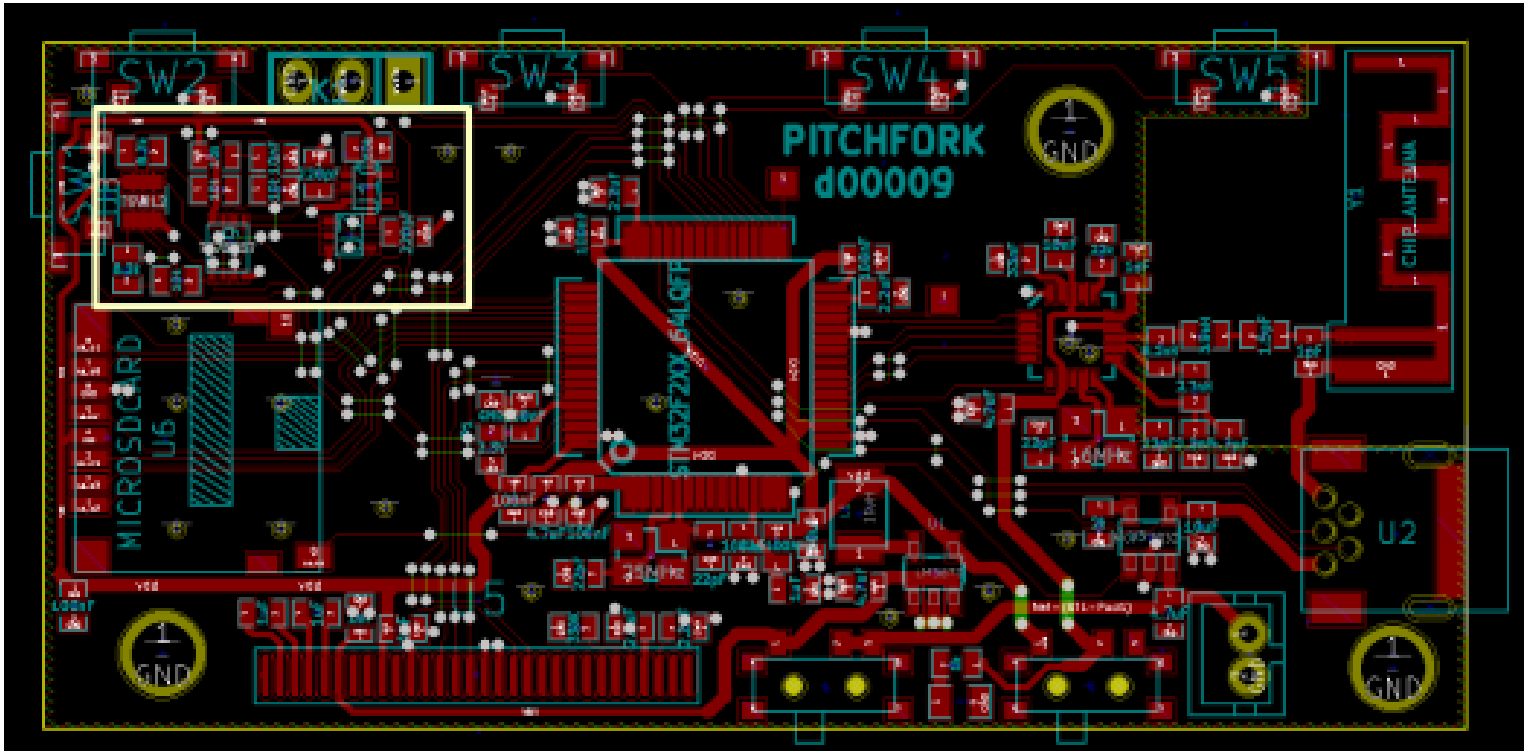
# 5 buttons


SW2
SW3
SW4
SW5
SW1
PITCHFORK
d00009
GND
MICROSDCARD
U5
U2
GND
GND

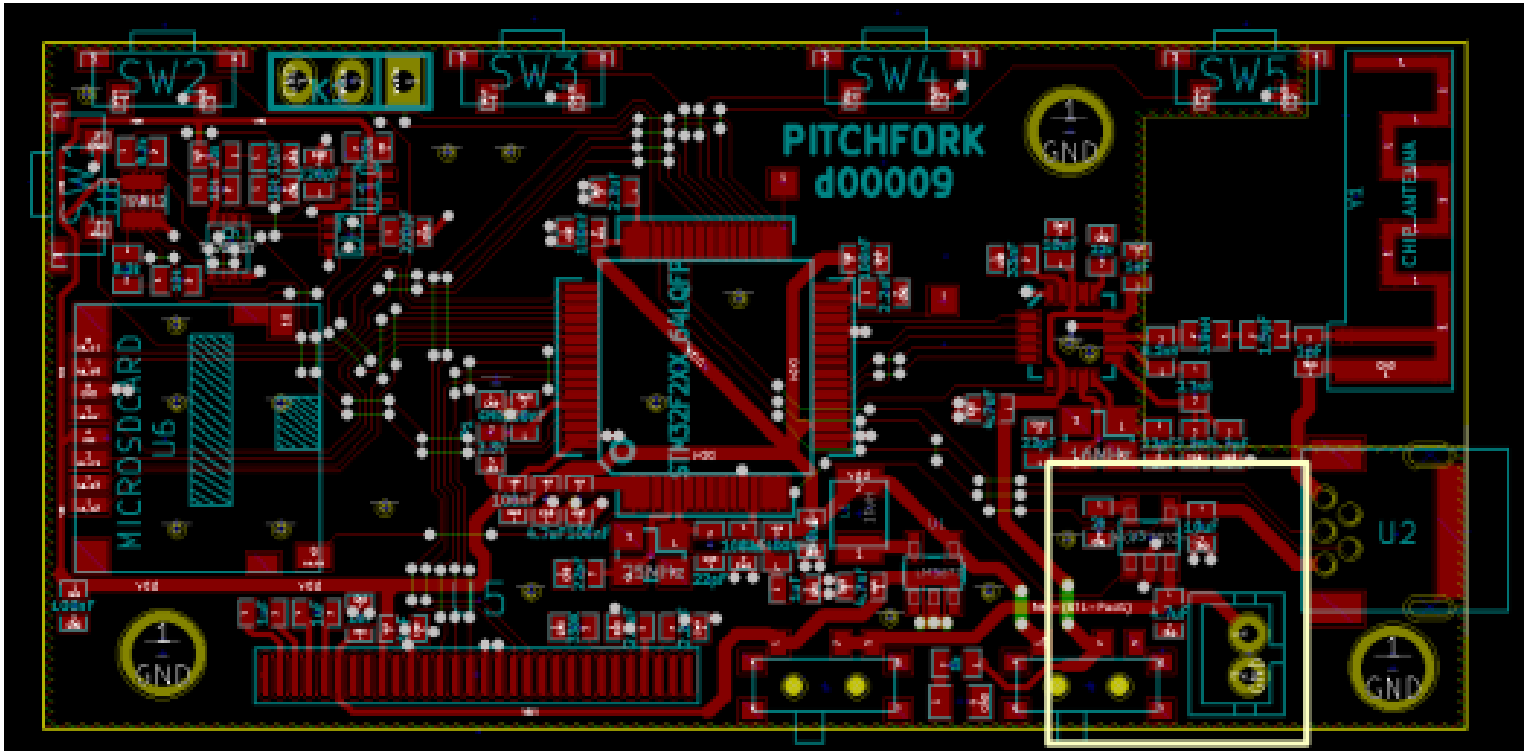
# 128x64 OLED


SW2
SW3
SW4
SW5
PITCHFORK
d00009
GND
MICROSDCARD
U5
U2
16MHz
CHIPANTENNA

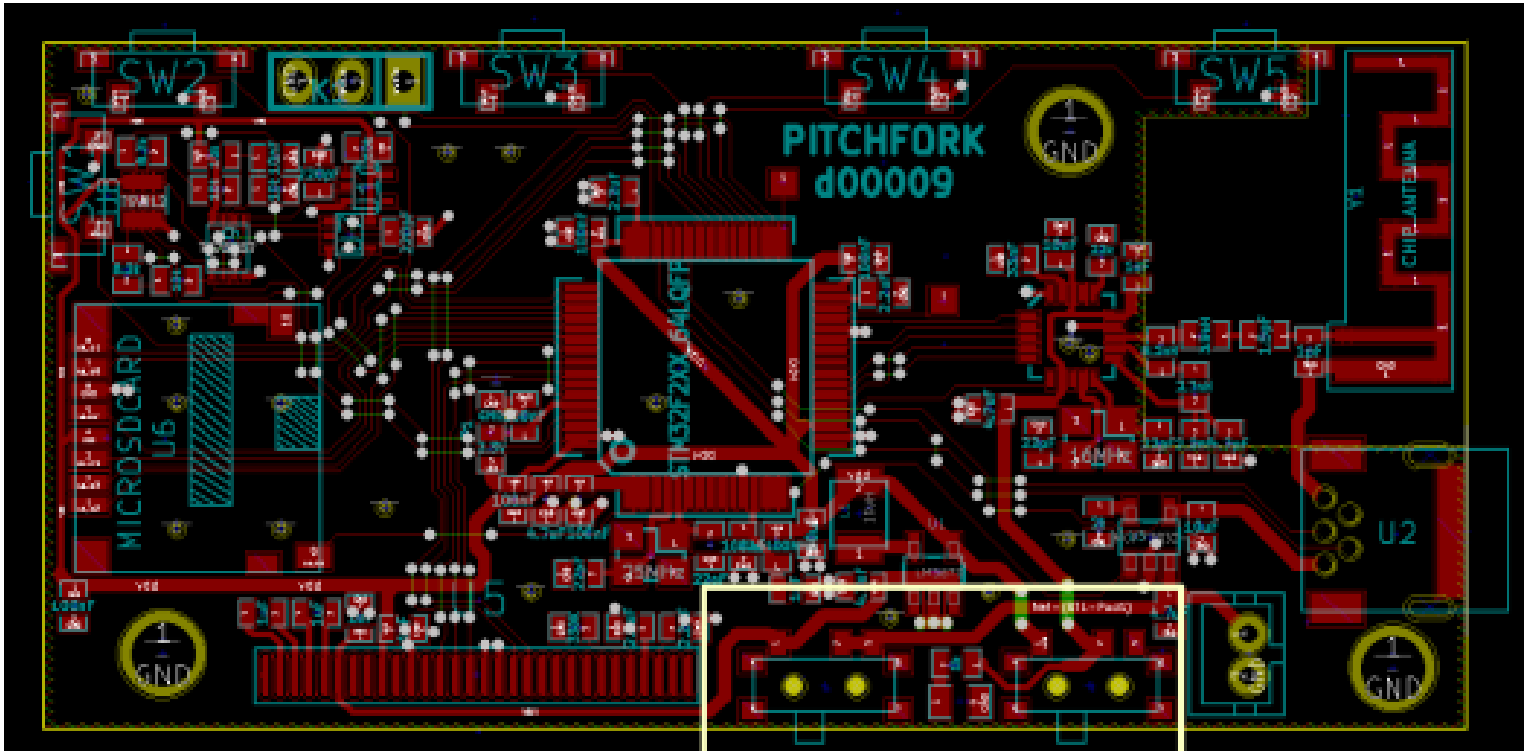
# external entropy source



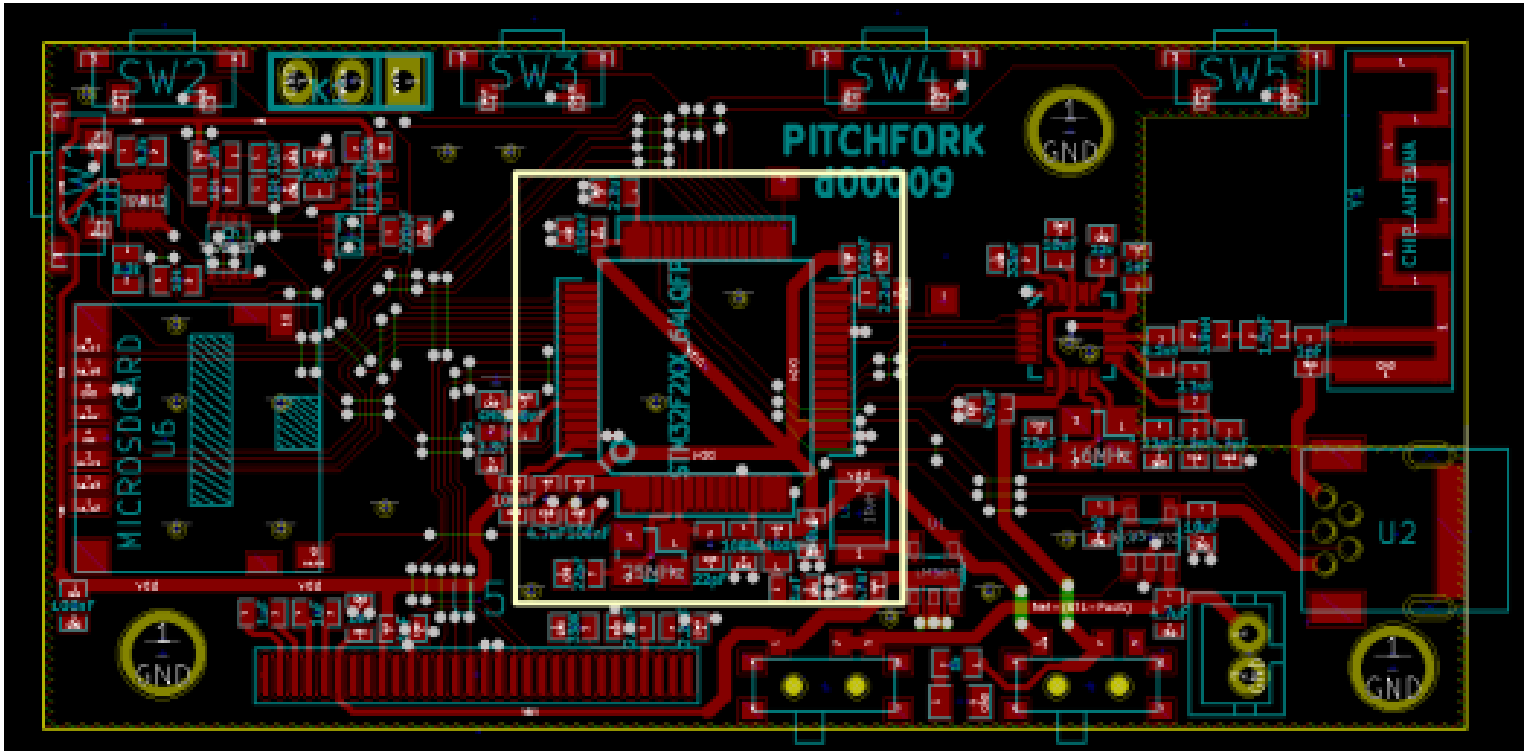
# battery + charger



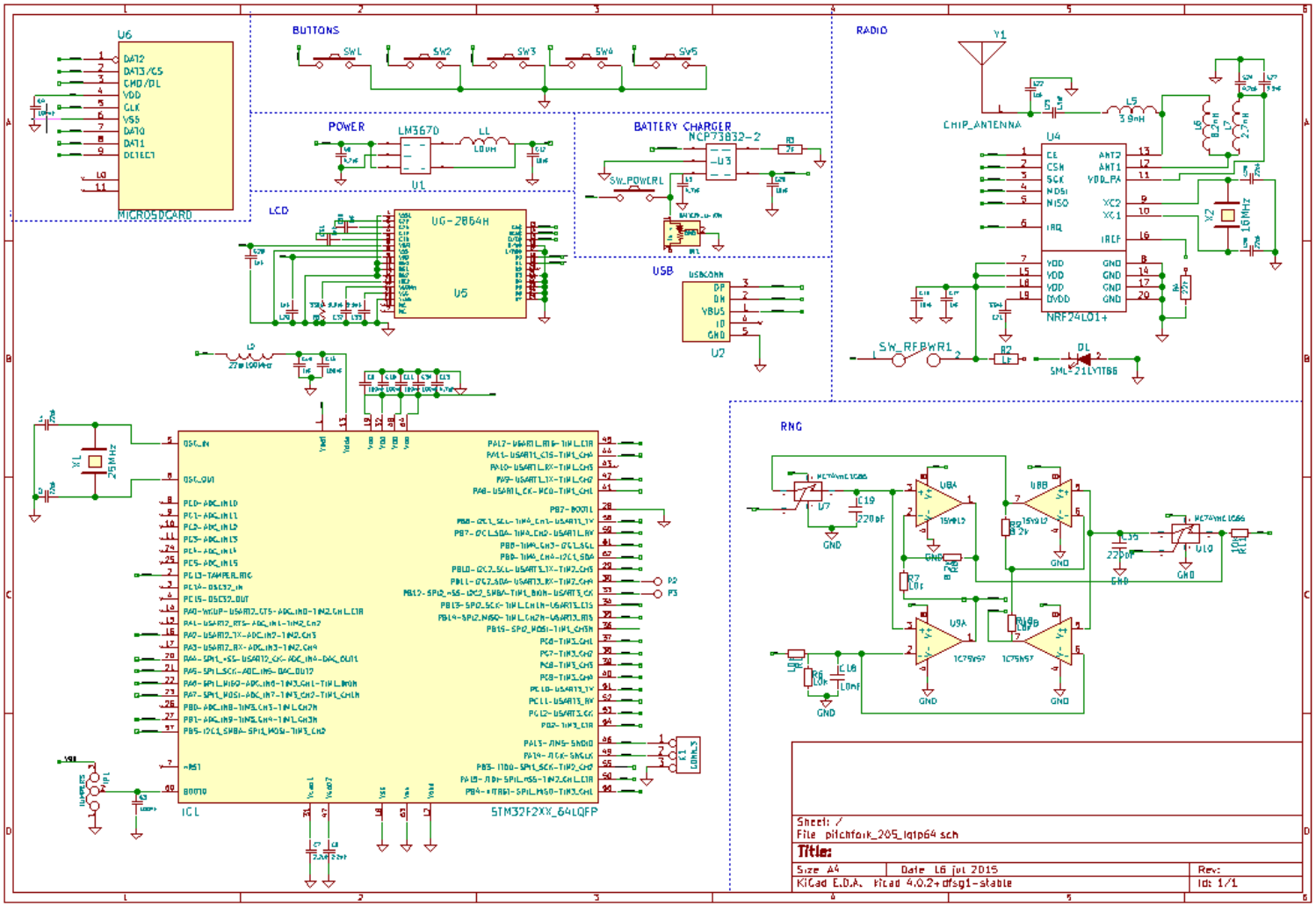
# switches


SW2
SW3
SW4
SW5
PITCHFORK
d00009
GND
MICROSDCARD
U5
U2
16MHz
GND
GND

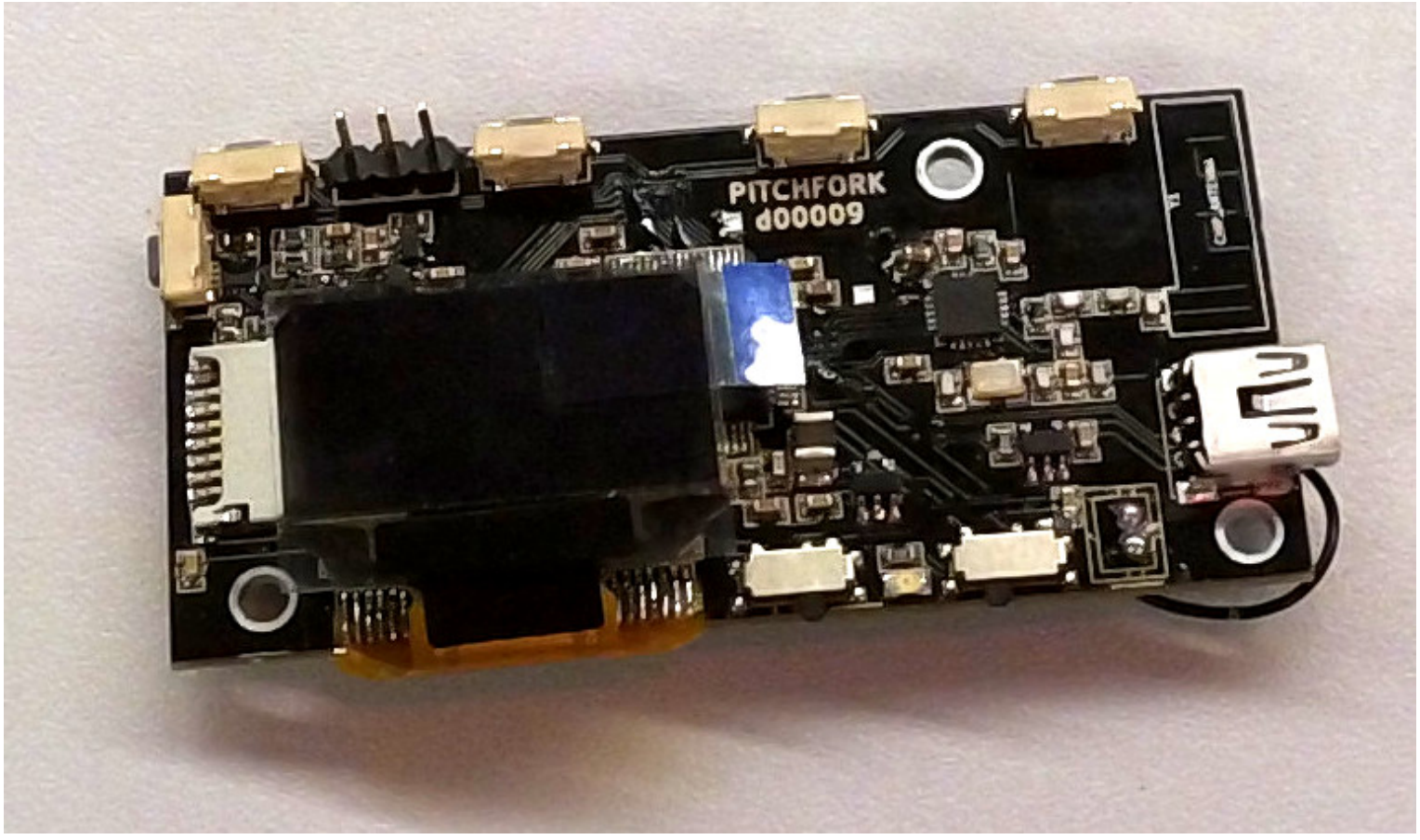
# and a cpu



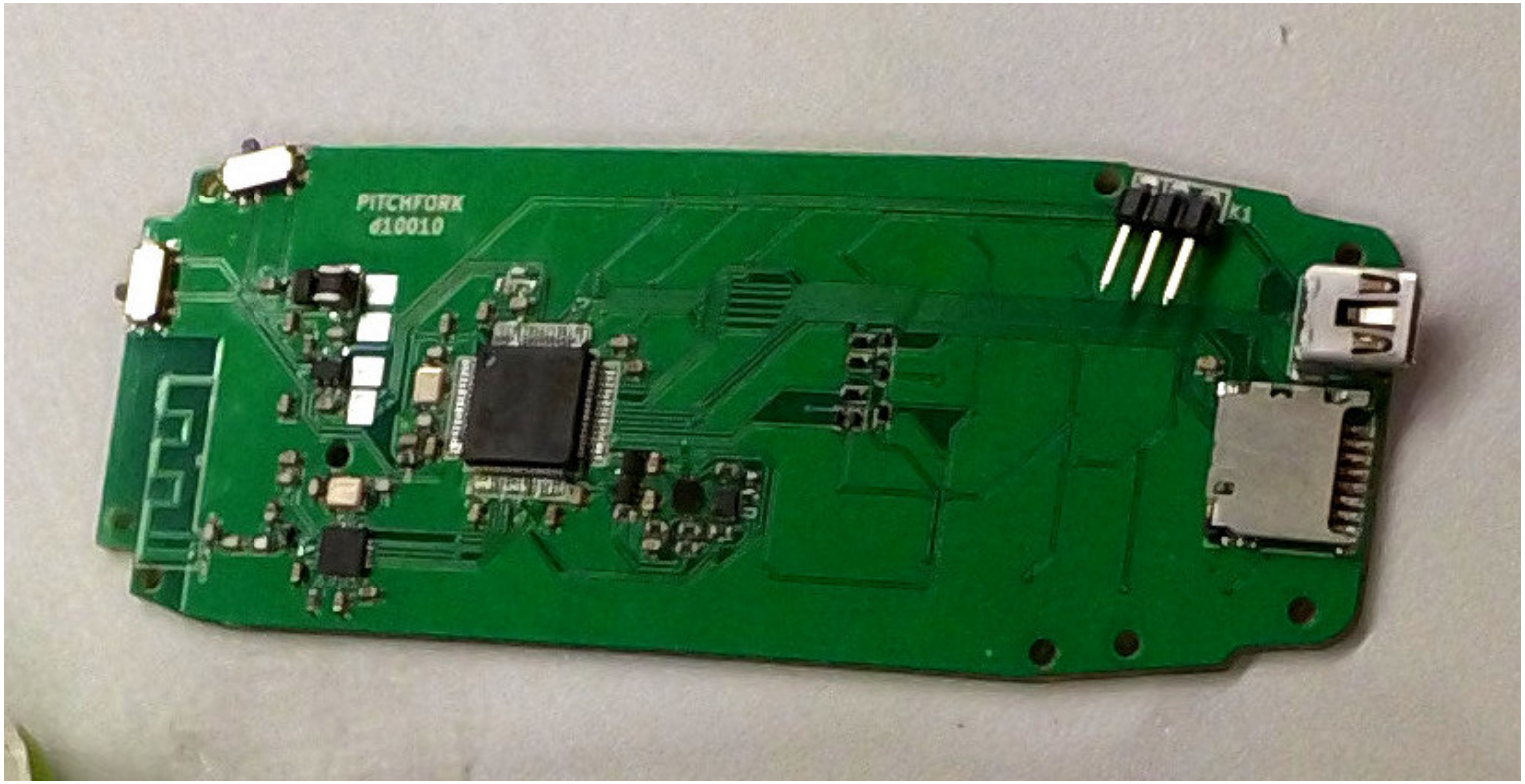
# guitarhero schematics



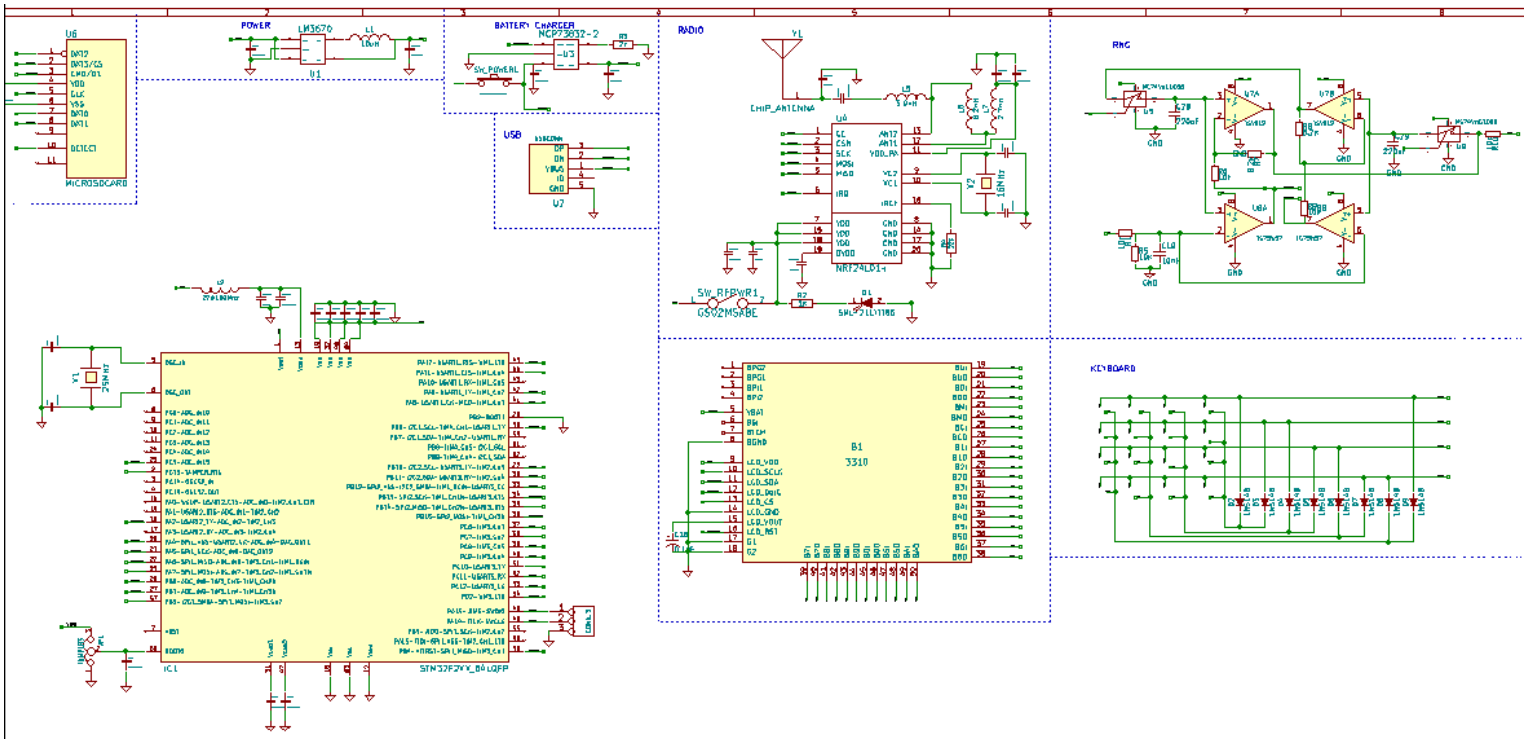
# guitarhero formfactor

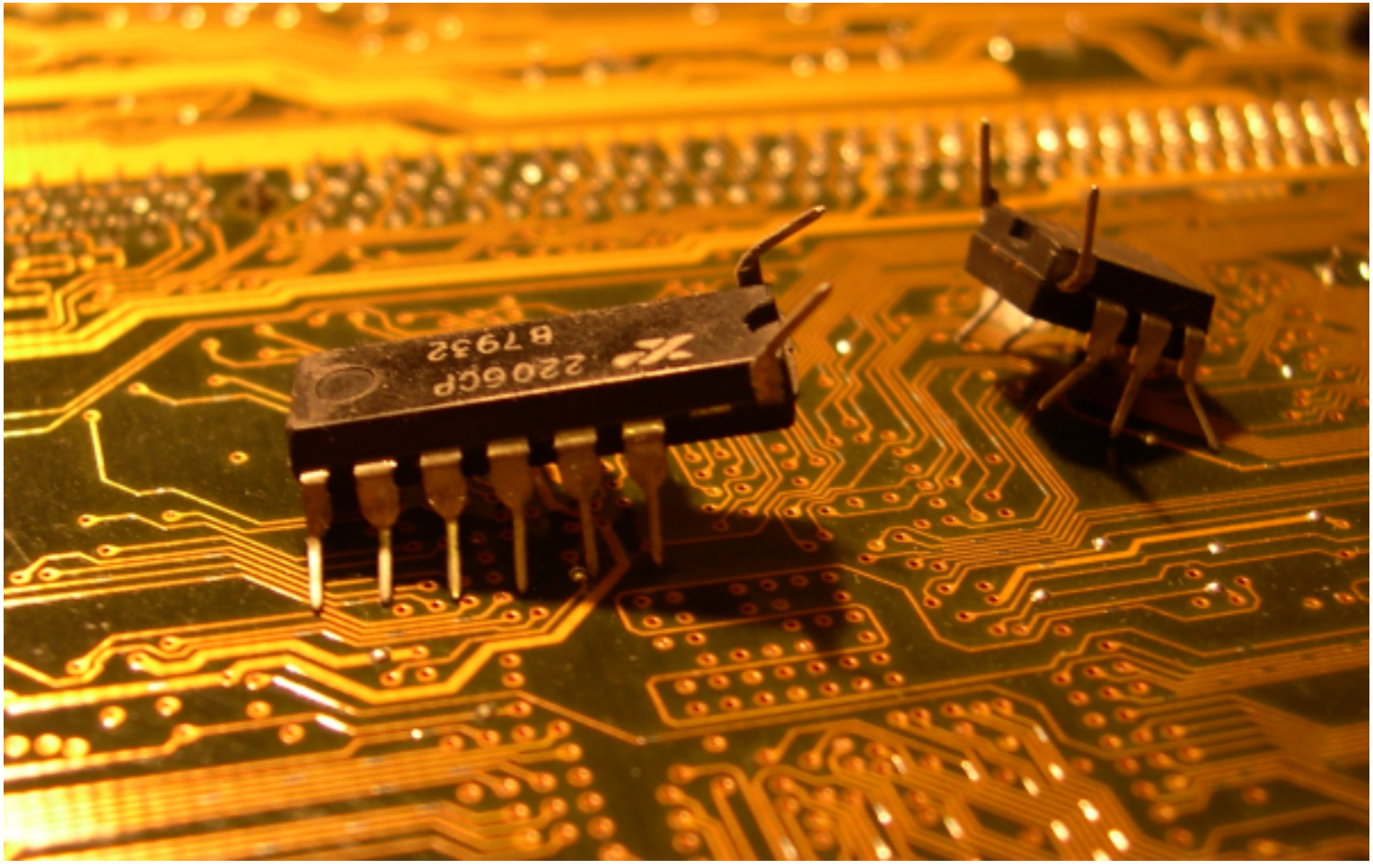


# alternative formfactor

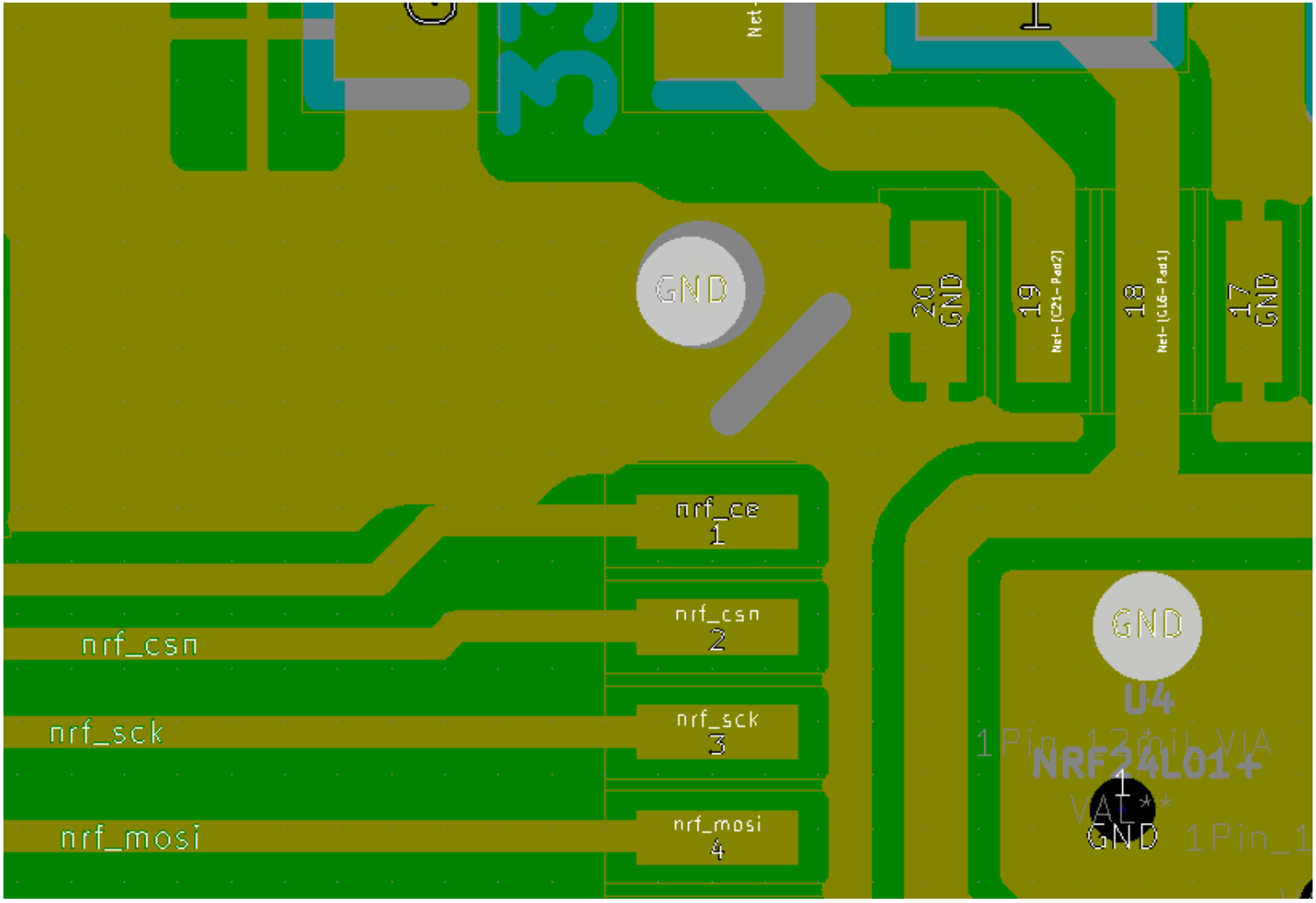


# nokia schematics

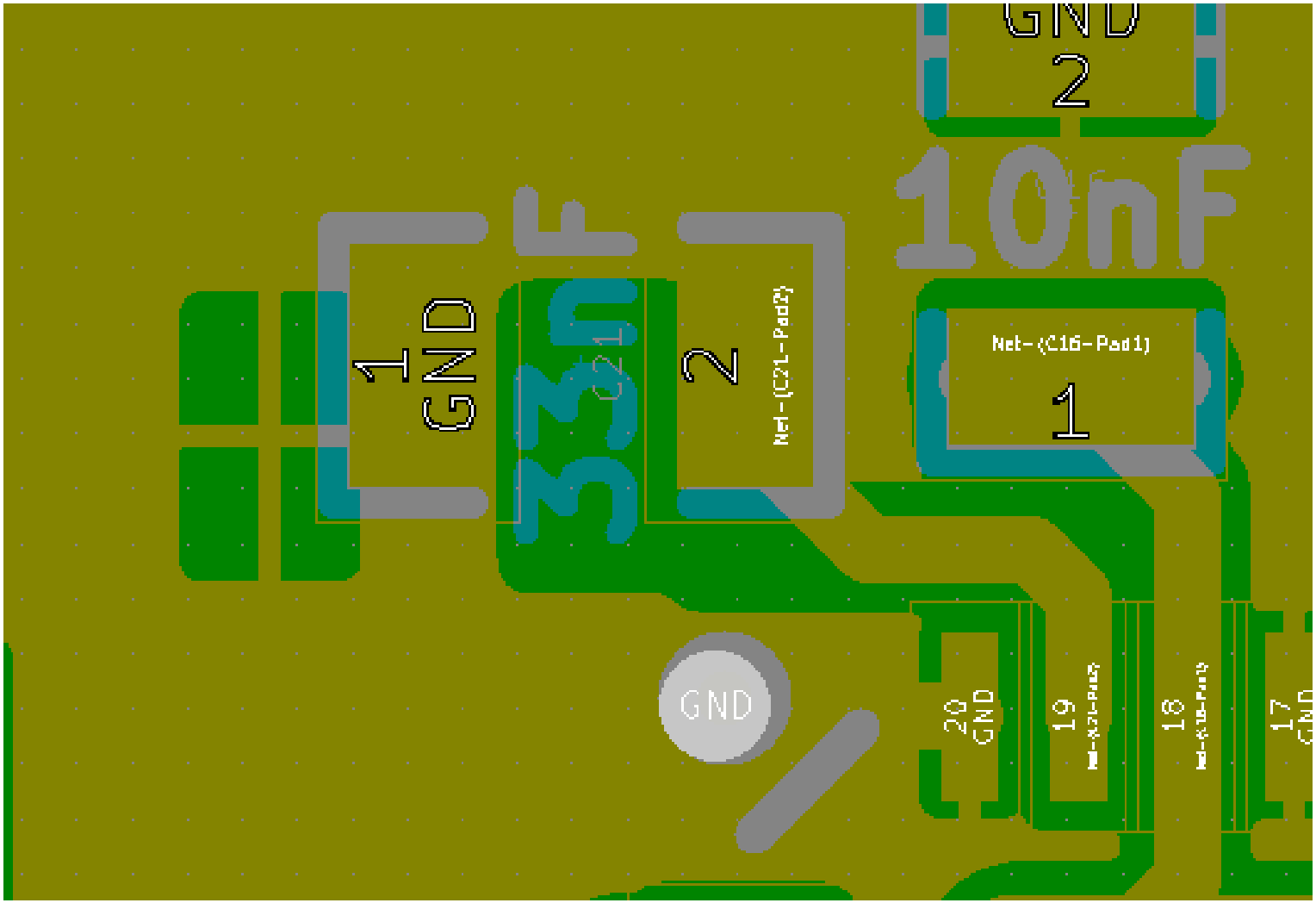



220GP
B7932

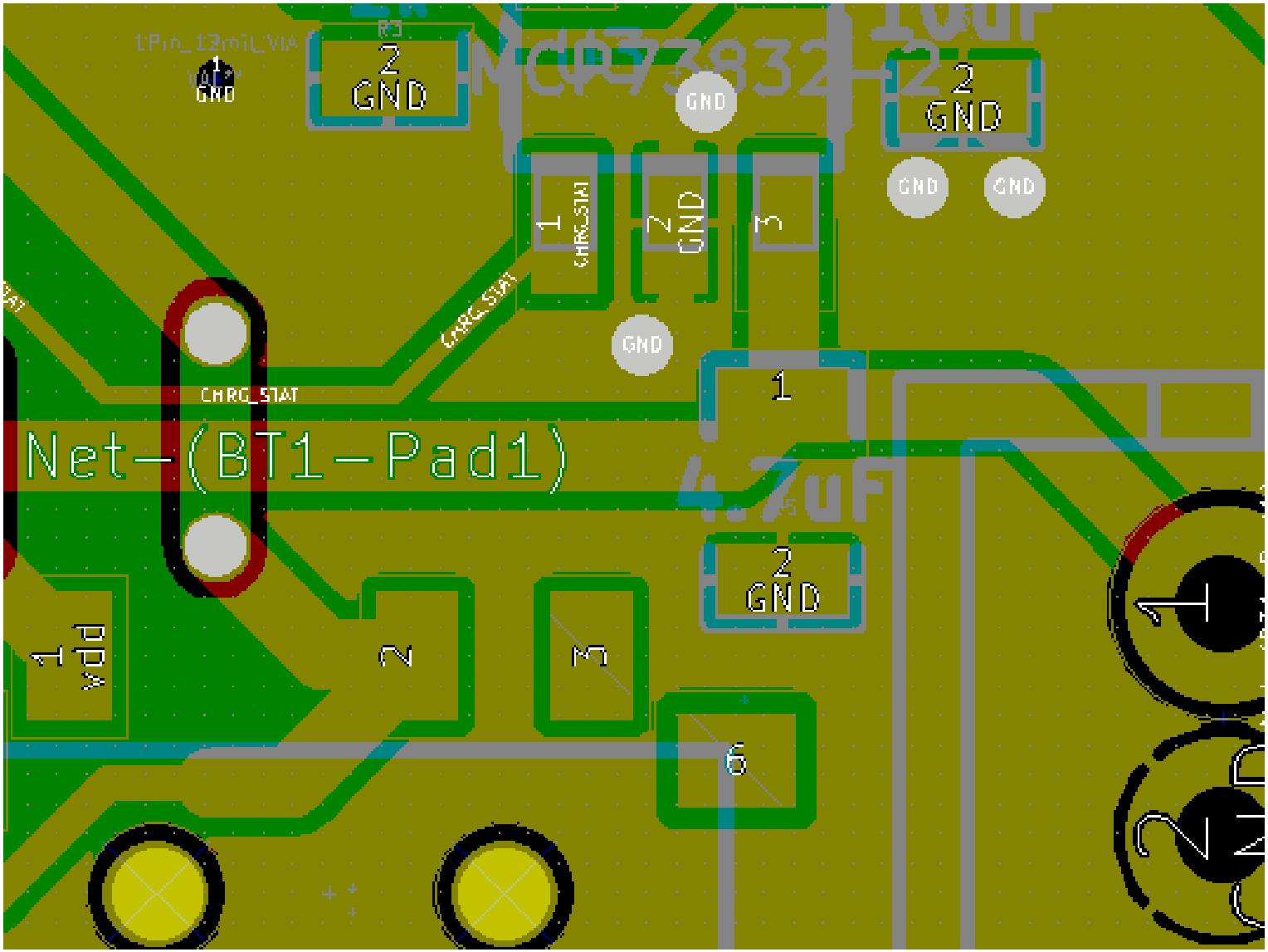
# bad zones


GND
20
GND
19
Net-(C21-Pad2)
18
Net-(C16-Pad1)
17
GND
nrf_ce
1
nrf_csn
2
nrf_sck
3
nrf_mosi
4
nrf_csn
nrf_sck
nrf_mosi
GND
U4
NRF24L01+
GND

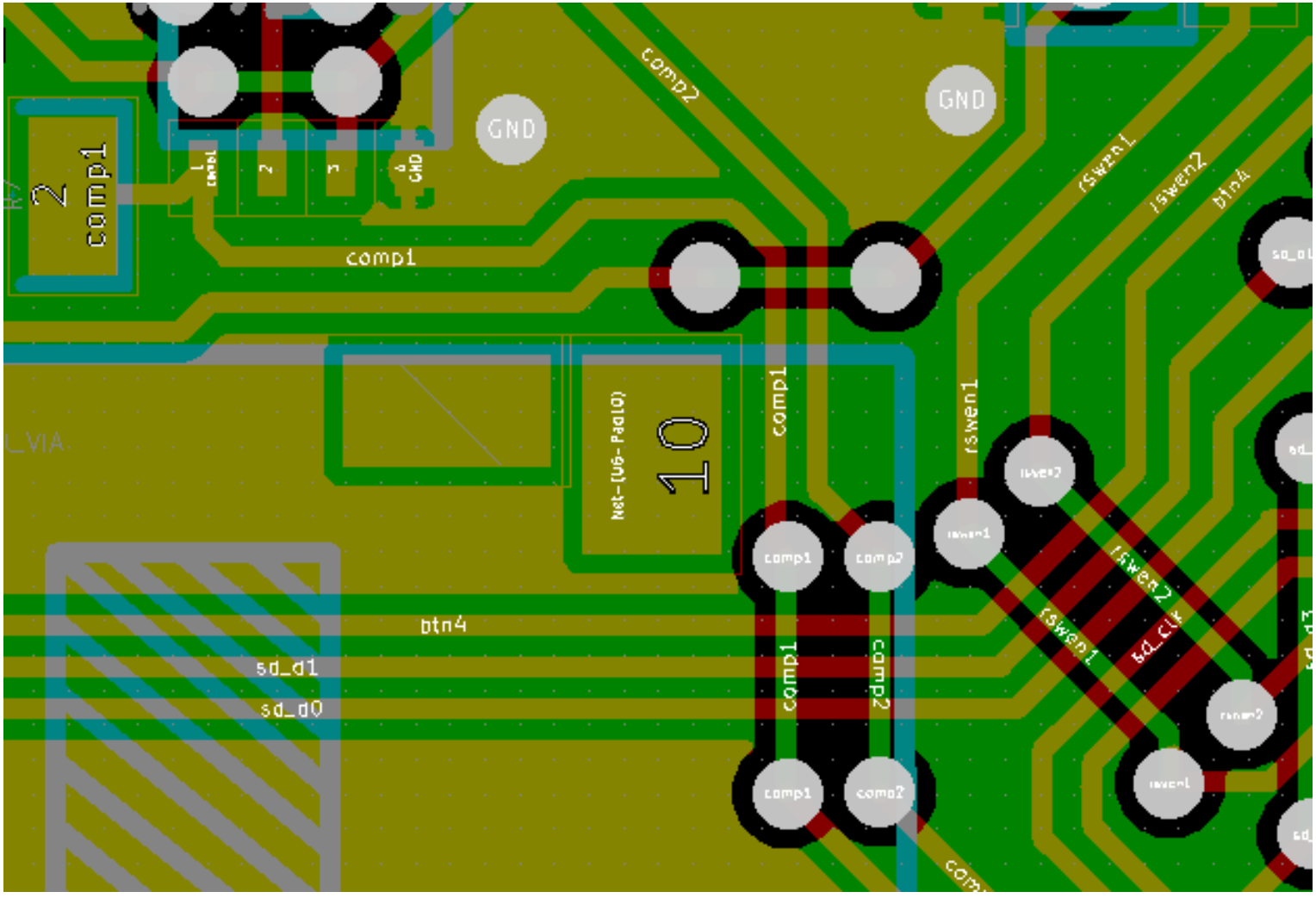
# bad zones


GND
2
10nF
GND
1
C21
2
Net-(C21-Pad2)
Net-(C16-Pad1)
1
GND
20
GND
19
18
17

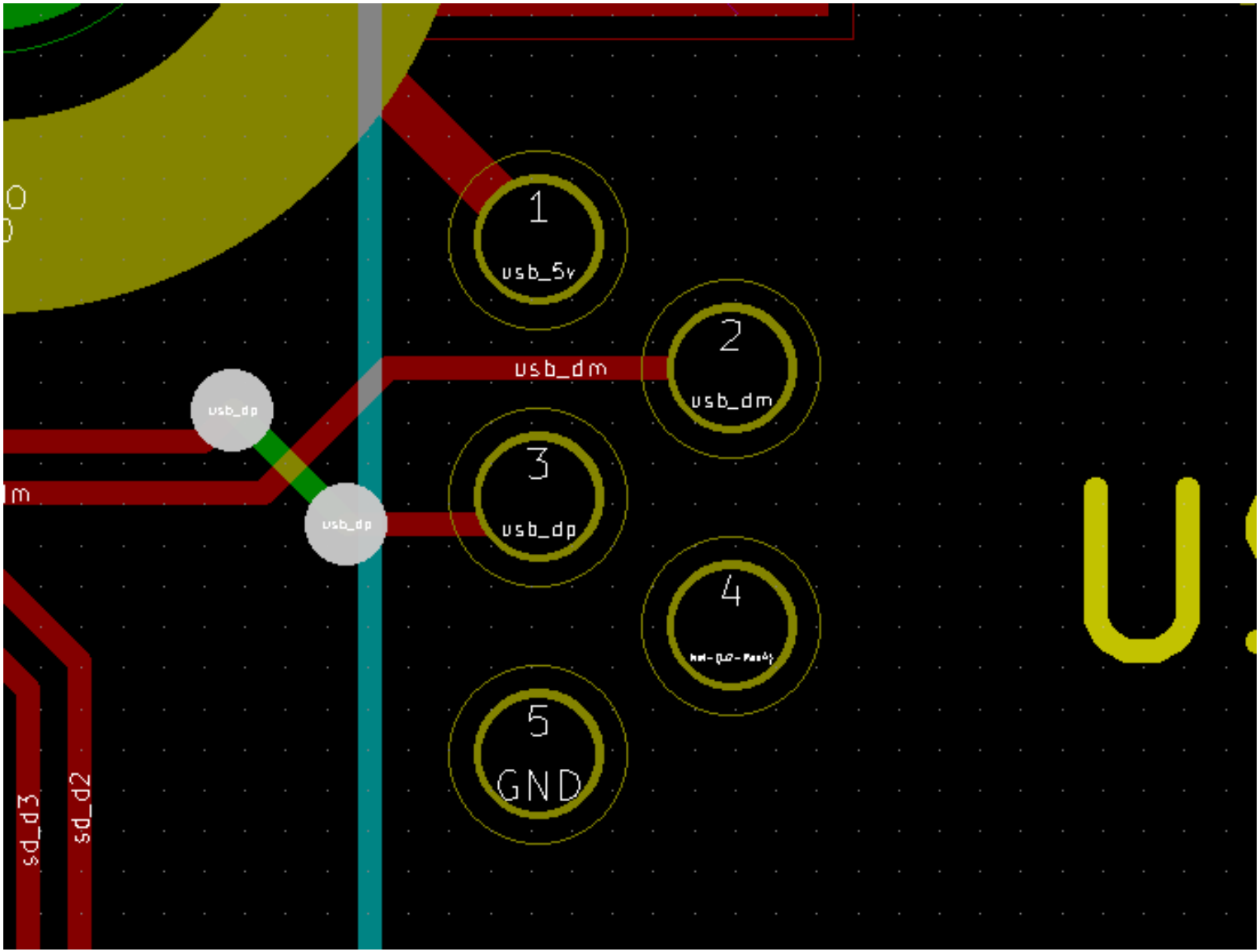
# missing resistor



# sd card detection



# usb on nokia board m(



# other nokia "features"

- nokia board thickness
- nokia needs LiPo battery, comes with NiCd :/

# features

- free software/hardware
- key exchange over 2.4GHz
- post-quantum crypto (newhope and symmetric)
- threat model
- mass-storage usb mode
- secret-key based: sign, encrypt, verify, decrypt
- python bindings

# general computing device

- display
- network
- usb
- buttons
- storage

demo time

planned features o7

# casing

# Perfect forward secrecy using Axolotl ratchet (PoC)

# Smartwatch form factor

# features

- HOTP, maybe also TOTP (experimental) (with new cpu)
- transparent block-level encryption onto sd cards
- post-quantum signing using sphincs (PoC)
- better UI on the PITCHFORK
- smartphone support
- gpg compatibility layer
- use some security m3
- Attribute based credentials
- password storage
- USB2.0 interface with DMA

# challenges /o\

- USB
- right-handed pitchfork /o\
- proper crypto
  - mapping uids to keys
  - KDF for the passcode
- proper filesystem /o\
- usable gui /o\

development

development
is fun!!!5!

# hw design

<3<3<3<3 kicad!!!5!<3<3<3<3

## SW

- gcc arm toolchain
- SWD debugger
- libopencm3
- libsodium
- liblzg

# off-spring

- libsaxolotl
- pysodium
- pbp
- saxolotl
- pyrsp
- reflowmaster2k+ deluxe pro

# crowdfunding

- for future r&d and a production run
- start of september

# workshop

- build it (soldering)
- hack it (sw)

# thanks

(in random order) Vic, asciimoo, dnet, the r0ket team, peter schwabe, boldx, roland, mo, peter stuge, erdem alkim, kares, bill waywardgeek cox , pavol, viola, jz, atoth

Questions