Wireless Hacking with 'HackCUBE'

Yunding Jian，Jie Fu，Chaoran Wang

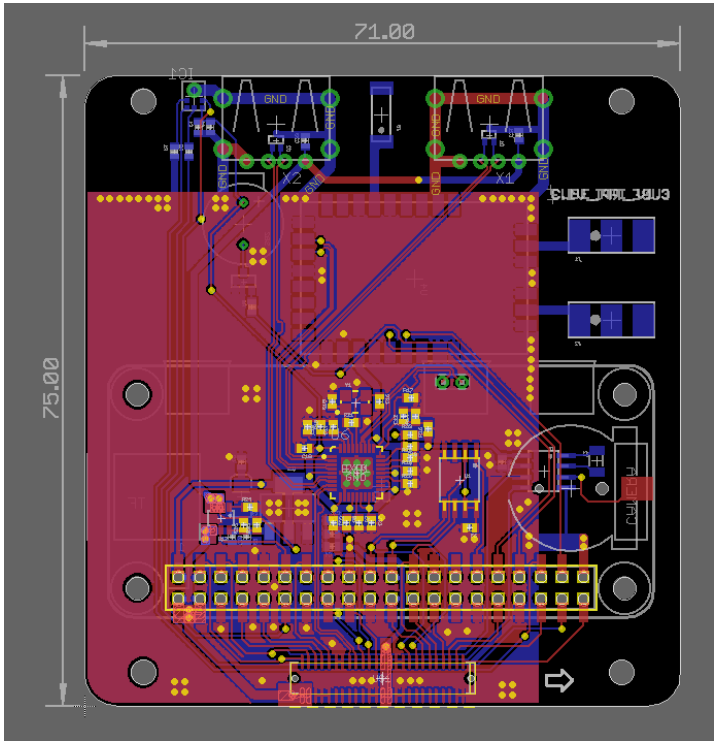
UnicornTeam, 360 Technology
April 1, 2018

What's the HackCUBE?

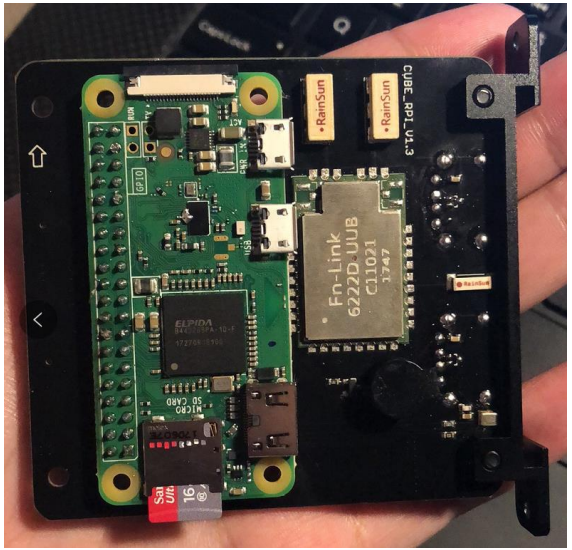
- HackCUBE is a hardware testing platform
- HackCUBE is a so opened platform
- HackCUBE is a well - designed and good - looking platform

The HackCUBE

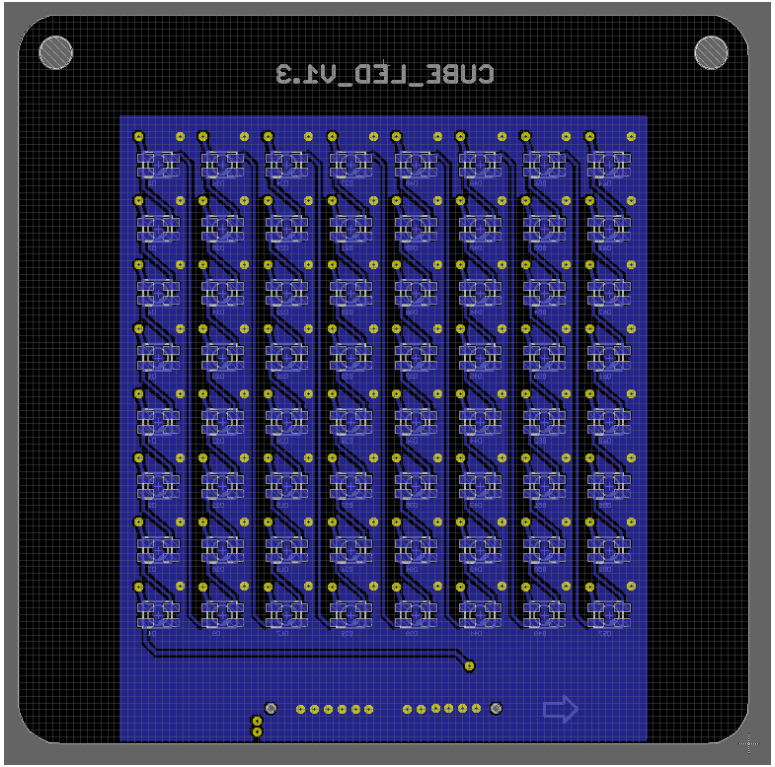
Core Board of HackCUBE



- Raspberry Pi Zero W
- USB2514B 4*USB HUB
- RTL8822BU 2.4G/5.8G WIFI
- DS1307 RTC
- SPI Flash
- Beep
- MIC

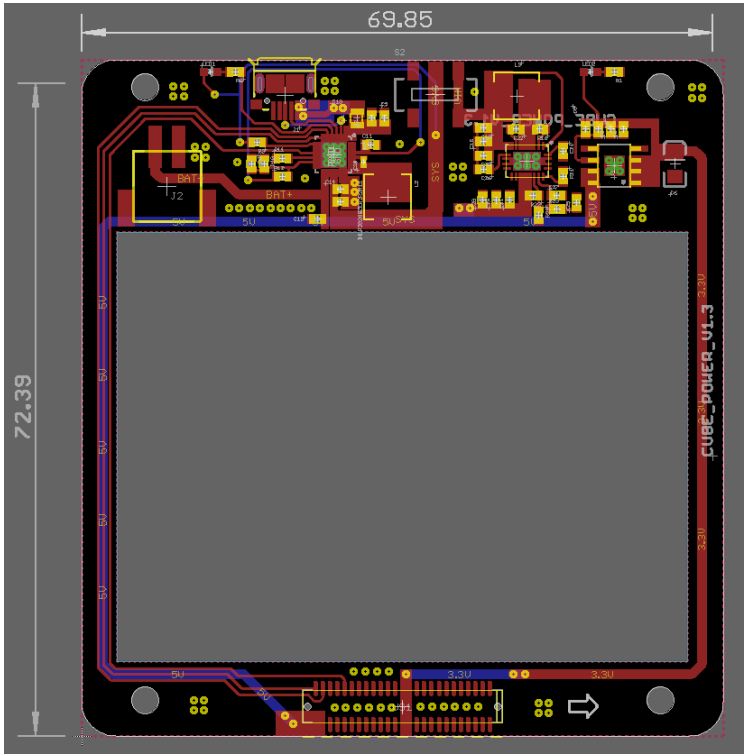


RGB LED Board



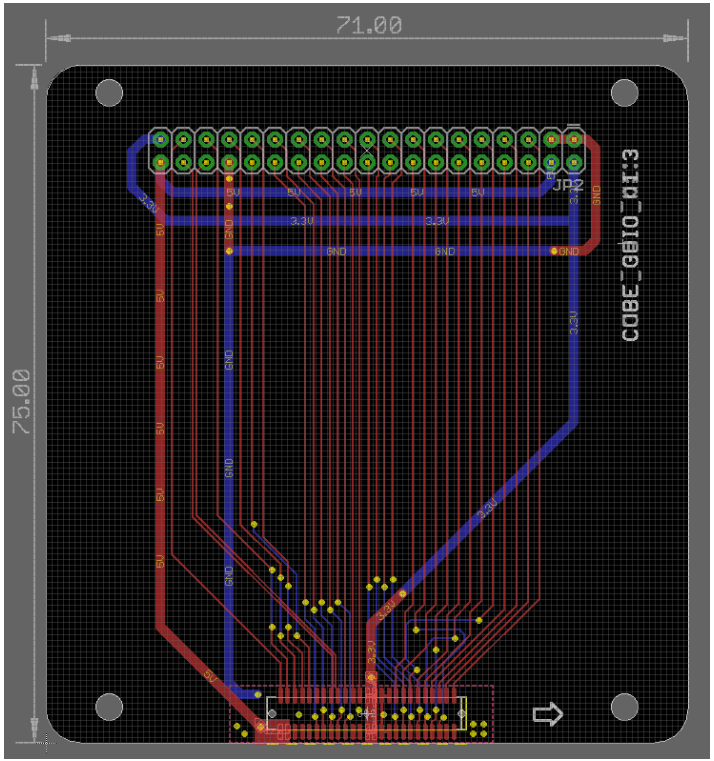
- 8*8 RGB LED
- Show Light
- Show Logo
- Flashlight

Power Board



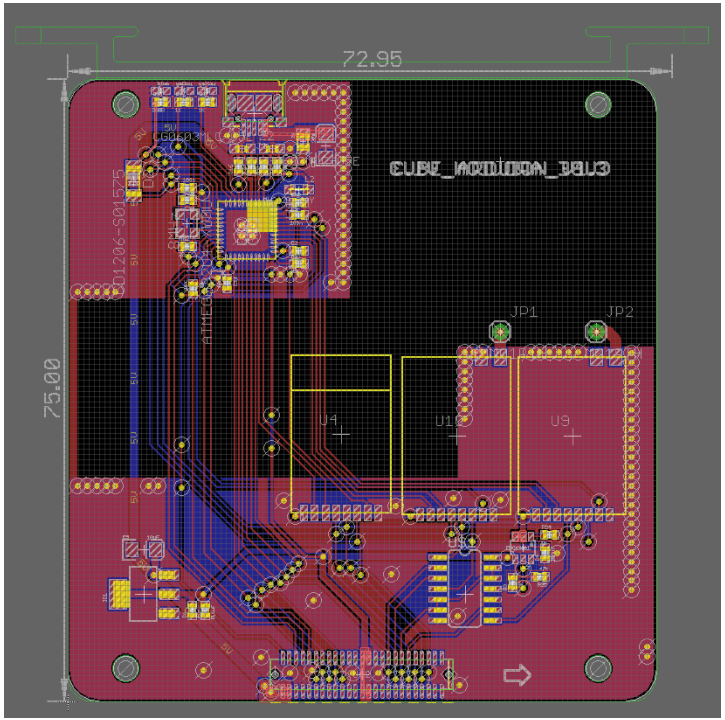
- TI BQ25895
  - Supports Max Charge (QC3.0)
- TI TPS61088
  - Boost to 5V

GPIO Board



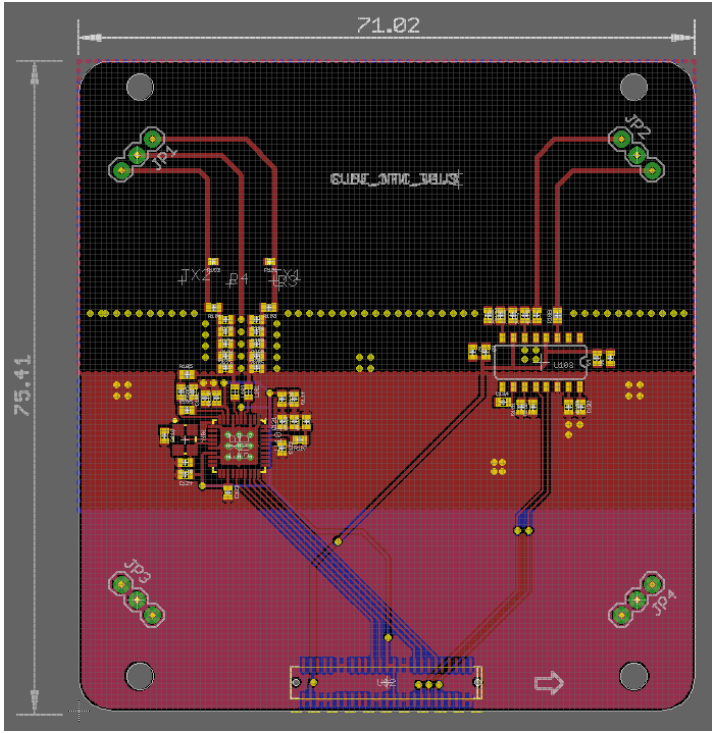
- ALL GPIO Extended

Arduino Board

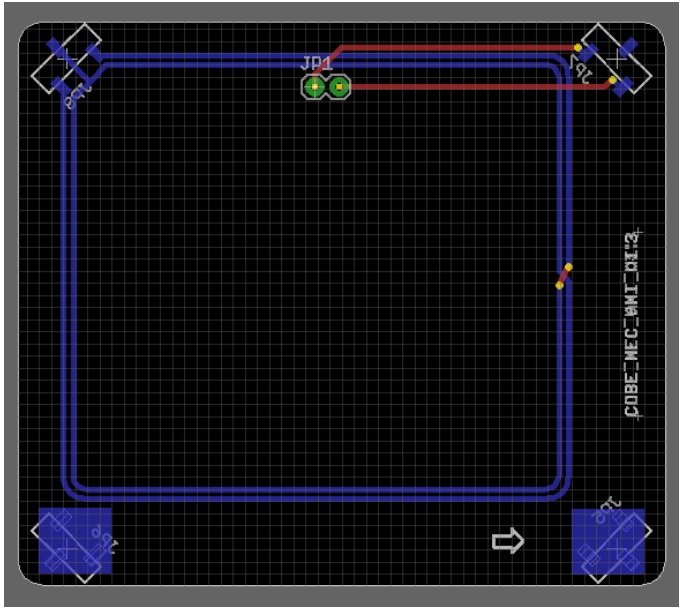


- Arduino Micro Pro 3.3V
- CC1101 433MHz
- CC1101 315MHz
- nRF24L01+ PA

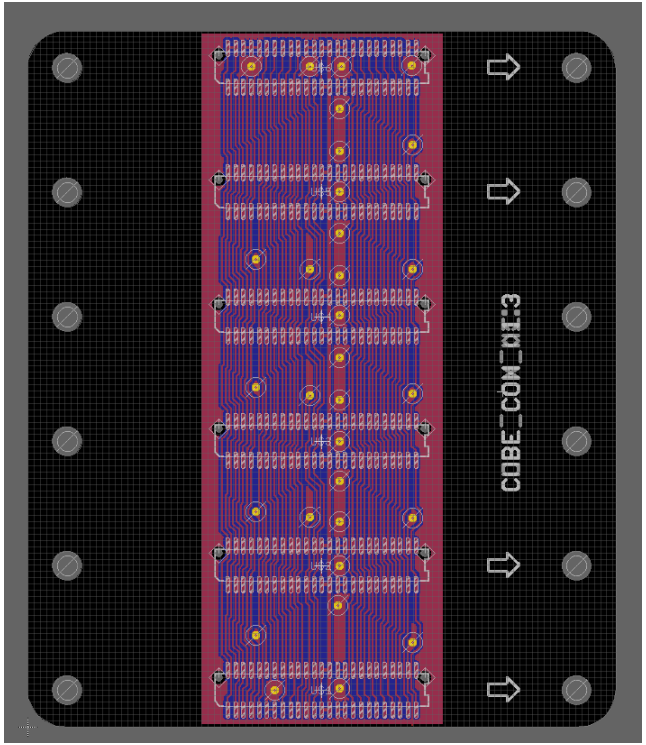
NFC & Anttan Board



- PN532
- EM4095

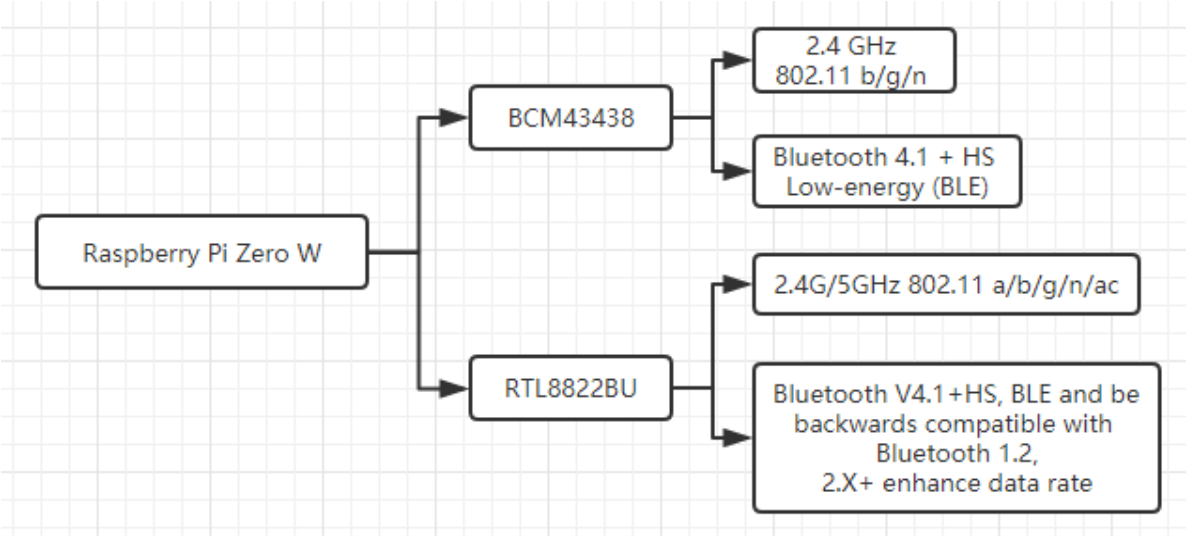


Connect Board



- 2*25P 0.8mm BTB Connector
- 6*Connector

What can we do: WIFI / BLE

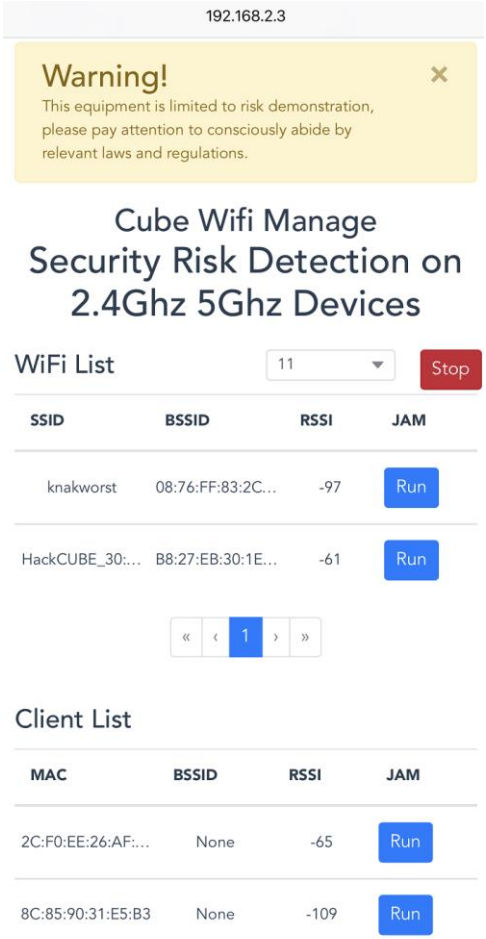


- WIFI Router
- WIFI Advertising
- WIFI Blocking Attack
- WIFI Fishing
- WIFI IOT Gateway
- WIFI …

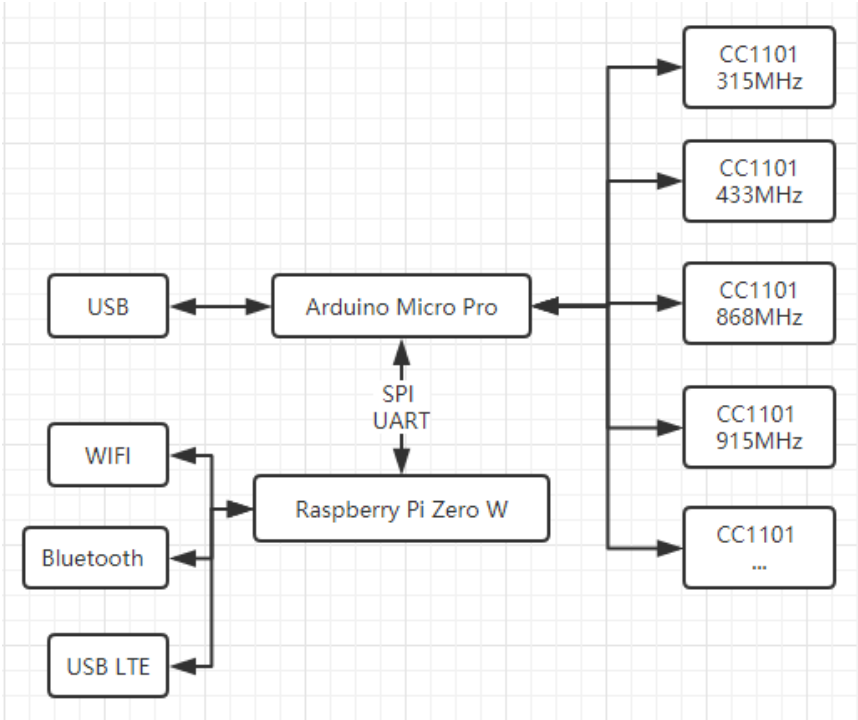
- Bluetooth Advertising
- Bluetooth Keyboard/Mouse
- Bluetooth IOT Gateway
- Bluetooth …

Demo 1: Wifi Attack

- WIFI AP: HackCUBE_xx:xx:xx
- WIFI Password: hackcube123
- Web Address: 192.168.2.3
- SSH User: root
- SSH Password: hackcube



What can we do: RF

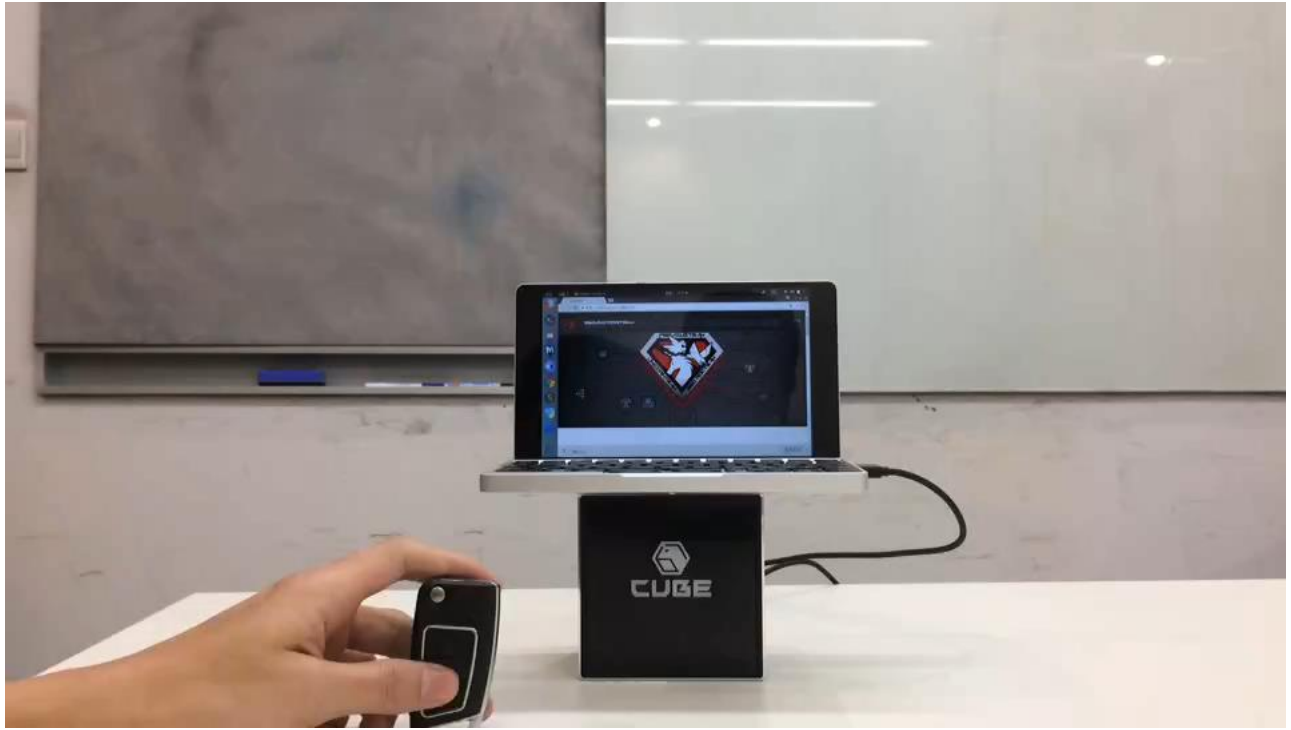


- IOT Sub-1GHz RF Board
- RFCat
- HID Attack Tool
- Remote Control Tool
- Wireless Keyboard
- RF Transmit Mode

Demo 2: RF Control Car

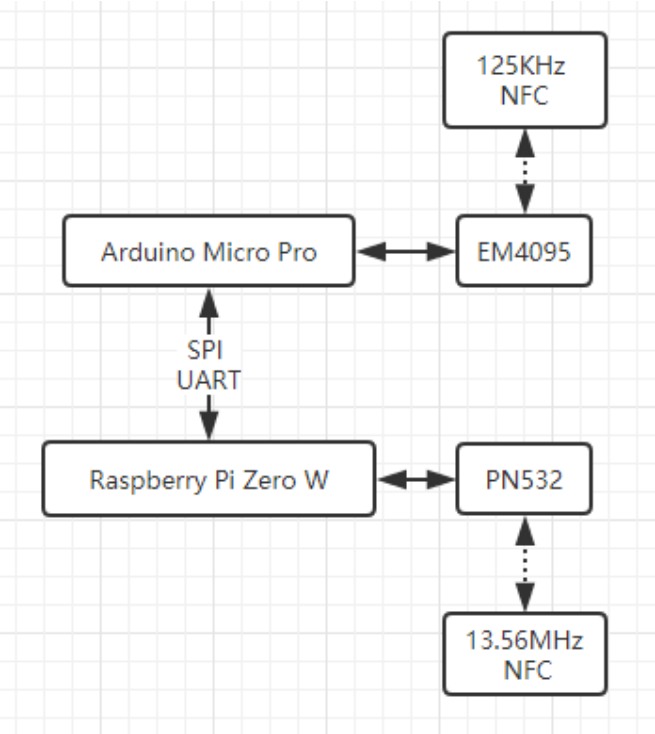
Demo 3: RF Control Quadcopter

Demo 4: Wireless Keyboard



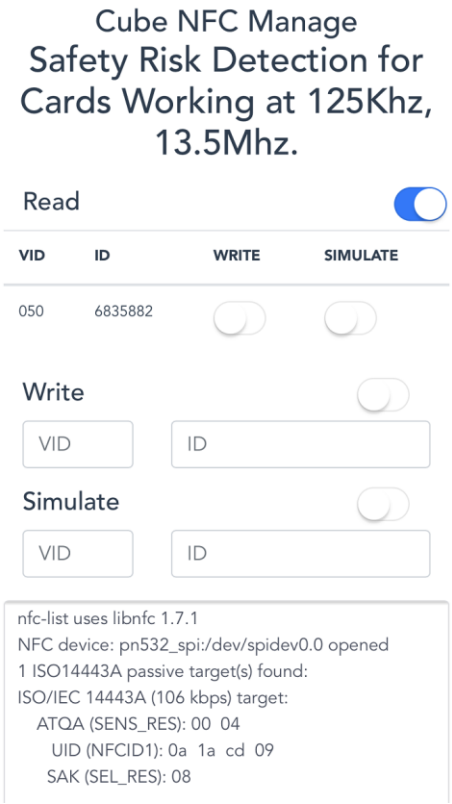
- Keyboard
- USB Network Card
- USB Disk
- BadUSB

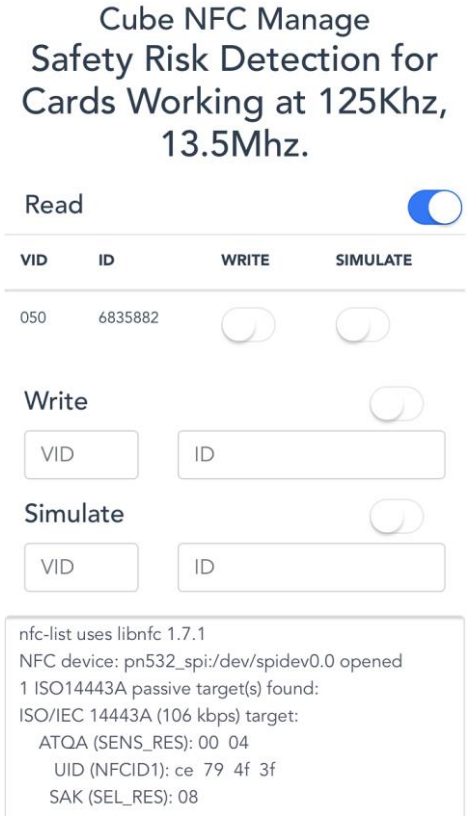
What can we do: NFC



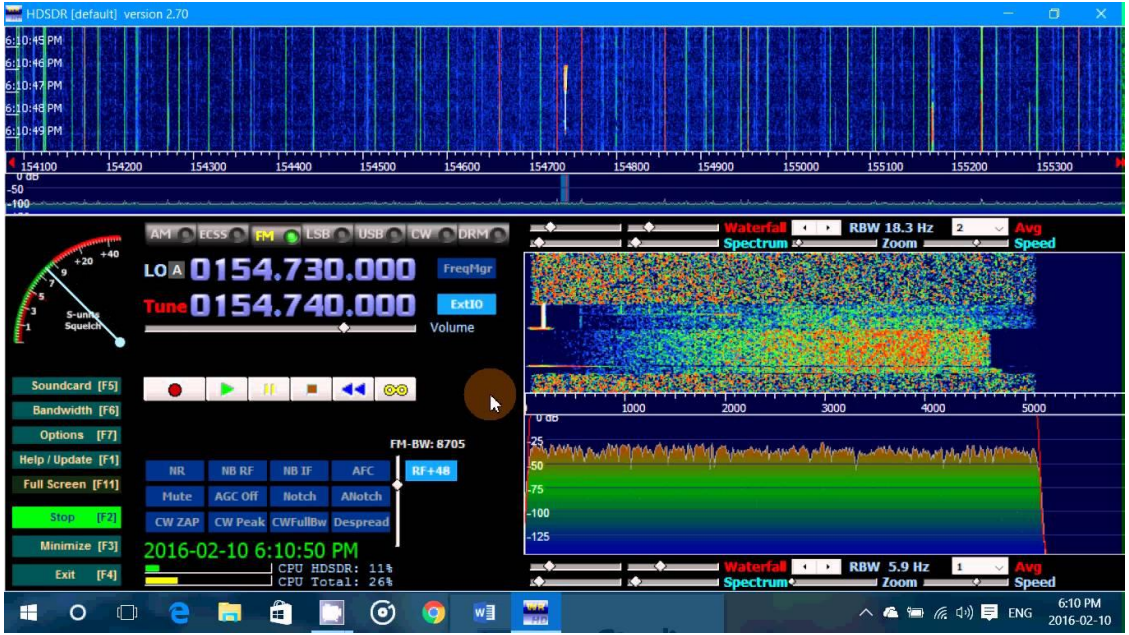
- 125KHz NFC Read/Write/Simulation
- Passive Keyless Enter
- 13.56MHz NFC Read/Write
- Crack Mifare Card

Demo 5: NFC Read/Write

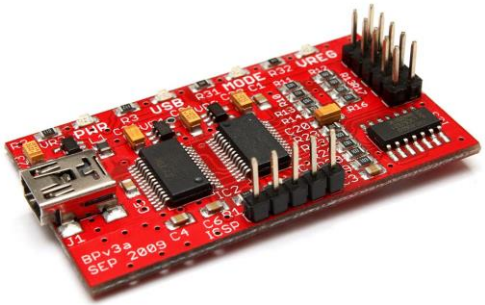




Our Plan: SDR

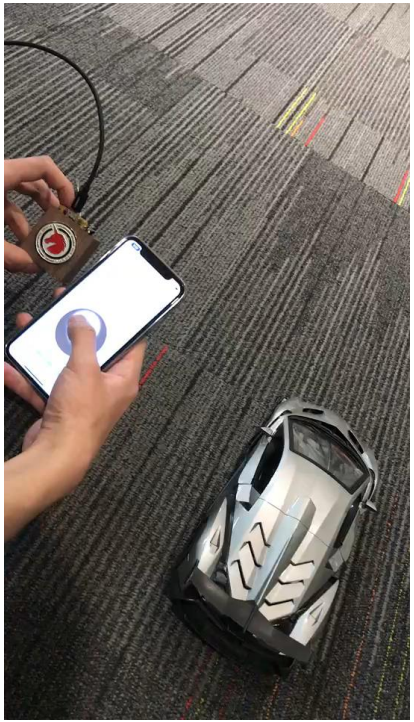

HDSDR [default] version 2.70
AM
ECSS
FM
LSB
USB
CW
DRM
LO A 0154.730.000
Tune 0154.740.000
FreqMgr
ExtIO
Volume
Soundcard [F5]
Bandwidth [F6]
Options [F7]
Help / Update [F1]
Full Screen [F11]
Stop [F2]
Minimize [F3]
Exit [F4]
FM-BW: 8705
NR
NB RF
NB IF
AFC
RF+48
Mute
AGC Off
Notch
ANotch
CW ZAP
CW Peak
CWFullBw
Despread
2016-02-10 6:10:50 PM
CPU HDSDR: 11%
CPU Total: 26%
Waterfall
Spectrum
RBW 18.3 Hz
Zoom
Avg
Speed
RBW 5.9 Hz
ENG
6:10 PM
2016-02-10

Our Plan: Debugger Tool



- OpenJTAG
- Buspirate
- CC Debugger
- Logic Analyzer
- IR Analyzer
- CAN Bus Aalyzer
- Zigbee Sniffer
- BLE Sniffer
- Other …

Next: HackCUBE Mini



- Small
- Portable
- High Intergration
- Low Price
- Other …

Next: HackCUBE Mini

- Small
- Portable
- High Intergration
- Low Price
- Other …

Next: HackCUBE Mini

- Small
- Portable
- High Intergration
- Low Price
- Other …

How to get it ?

https://github.com/UnicornTeam/hackcube.git

HackCUBE Pre-Order

Only limited units for USD299

The official release will be USD399

Option 0: Price are without USD50 shipping cost. World wide.

Option 1: Pay now and collect at #HITB2018SG USD299 NETT

Thank You ~