ECE 445 Spring 2021 Final Presentation

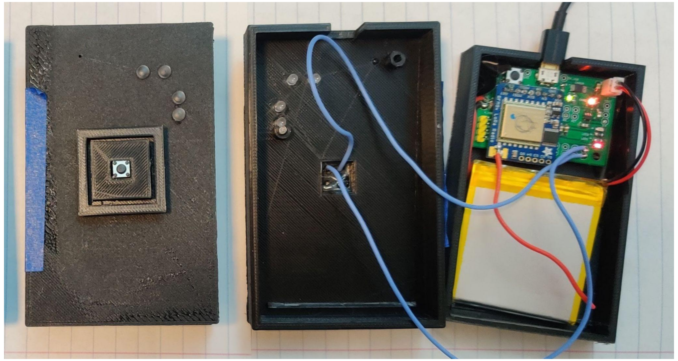
Covert Communications Device

Team 9
Braeden Smith
Ahmad Abuisneineh
Srivardhan Sajja

Introduction

- ➔ Wearable, secure covert communication device
- ➔ Sensitive military and law enforcement operations
- ➔ Allows for 1-to-many communication

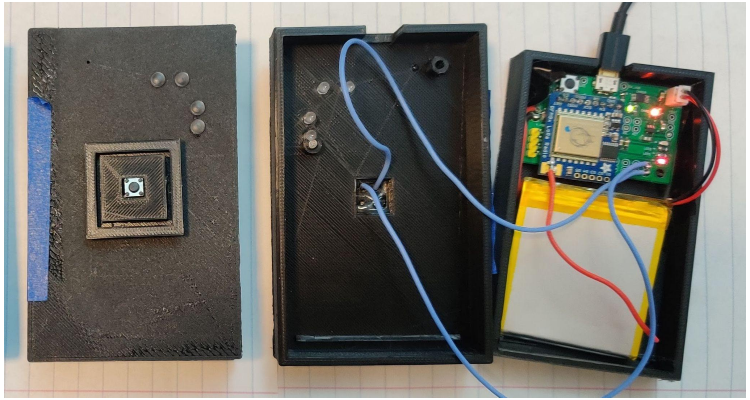
Typical application of end product



Device: PCB + Battery + Buttons + Case

Objectives

- ➔ Practical
  - Long range (1 km)
  - Battery powered
  - Easy to use
- ➔ Stealthy
  - Compact size
  - Quiet
- ➔ Secure
  - Cryptographic standards
- ➔ Fast
  - Short transmission time (2 secs)



Unopened casing with exposed button (left)
Opened casing with PCB & battery visible (right)

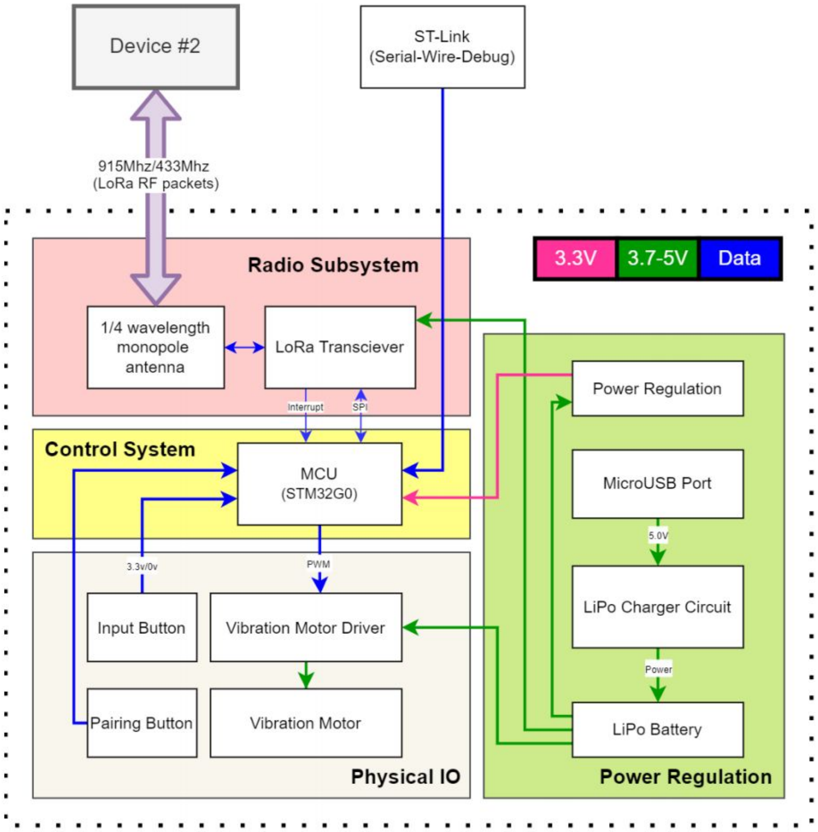
High-Level Requirements

- ➔ **1km** communication, Line-of-Sight
- ➔ Maximum of **two seconds** delay between button press and vibration felt
- ➔ Device may remain powered for at **minimum 8 hours**, and runs at maximum power output for at **minimum 1 hour**

Design

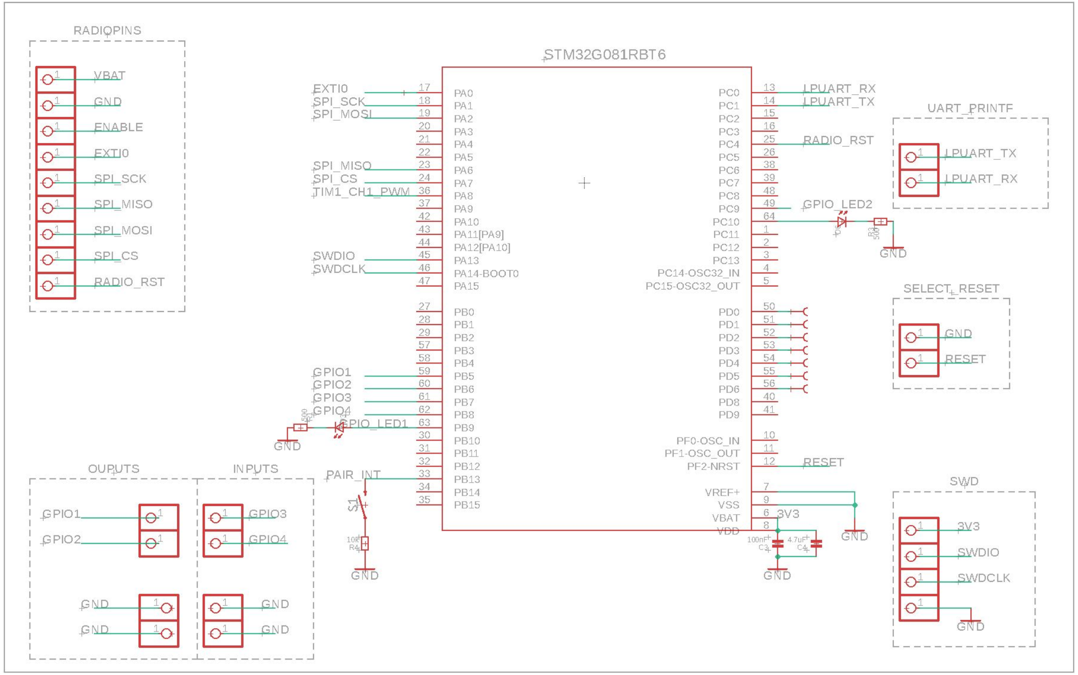
System Blocks

- ➔ Control System
  - ◆ Microcontroller (MCU)
- ➔ I/O
  - ◆ Input and Pairing buttons
  - ◆ Vibration motor
  - ◆ Motor controller
- ➔ Radio
  - ◆ LoRa Radio (915 MHz)
  - ◆ Antenna
- ➔ Power
  - ◆ LiPo battery (1200 mAH)
  - ◆ Linear regulator
  - ◆ Battery charger
  - ◆ Micro-USB port

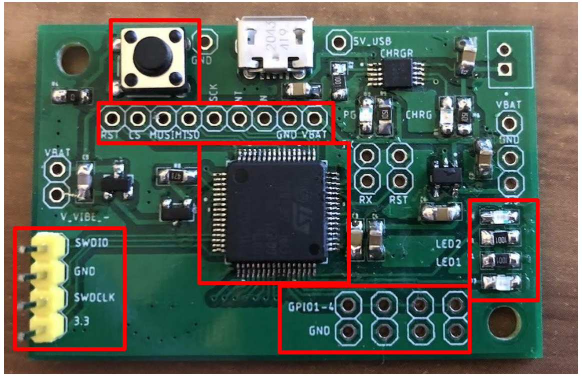


Complete block diagram for project

Schematics: Control System

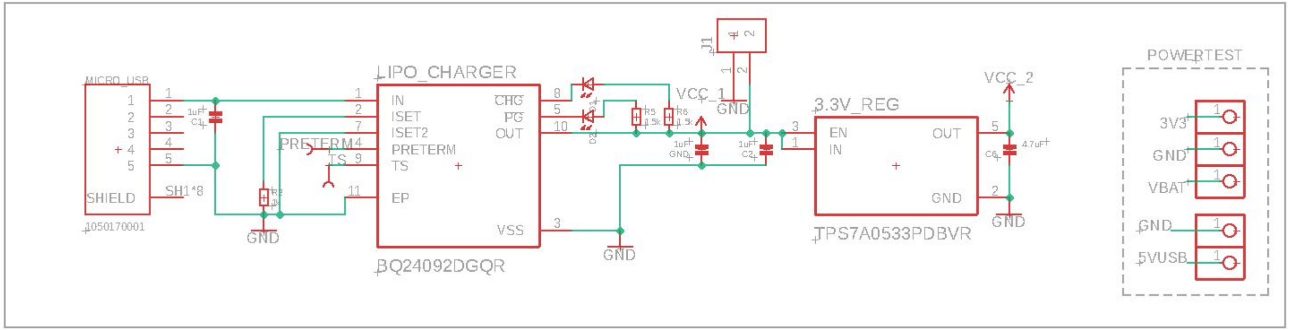


Detailed schematic of the control system

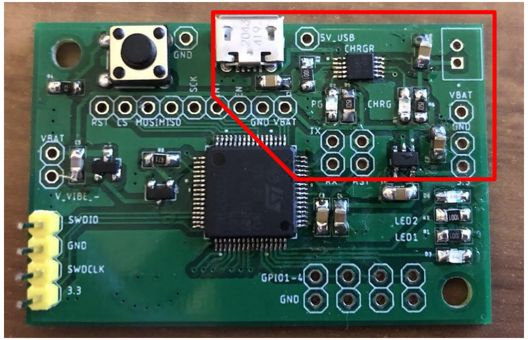


Control system on PCB

Schematics: Power System

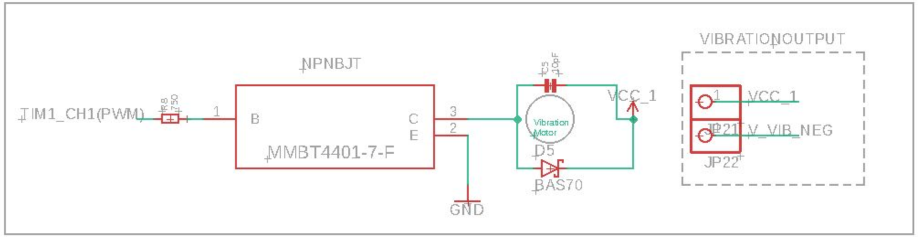


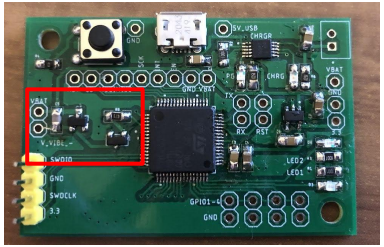
Detailed schematic of the power system



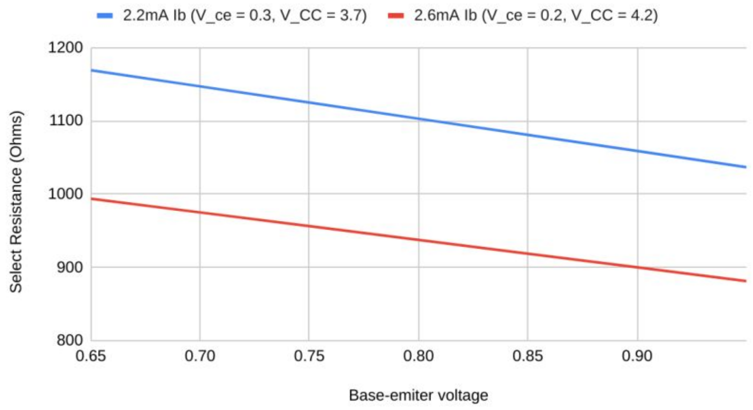
Power system on PCB

Schematics: Vibration Motor + Driver





Detailed schematic of the vibration motor and driver



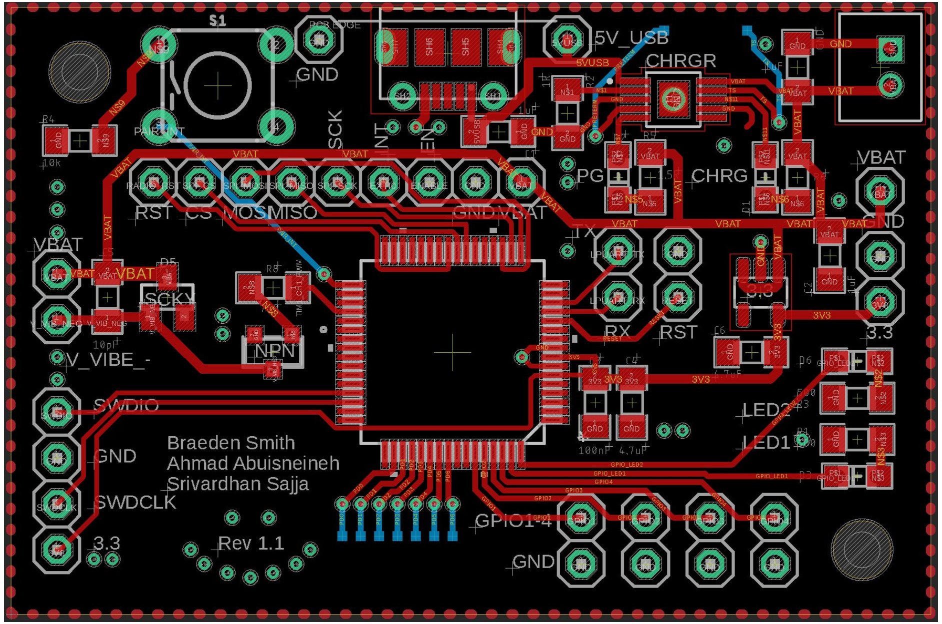
Models of Max+Min Voltage Drop Across the Load and the Resistors Available

$$V_{CE} = V_{CC} - I_C R_{Load}$$

$$I_C = \beta I_B$$

KVL Equations for an NPN transistor, used to determine ideal base current

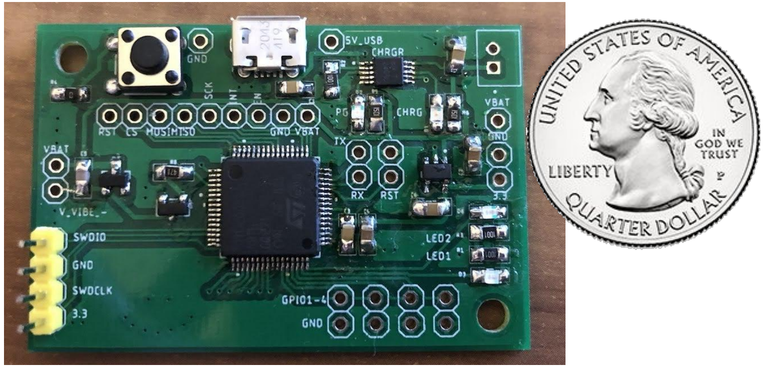
Schematics: PCB



1.32 inches

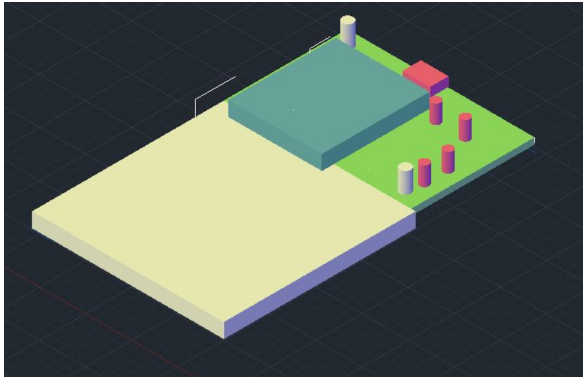
2 inches

PCB design made using Autodesk Eagle®

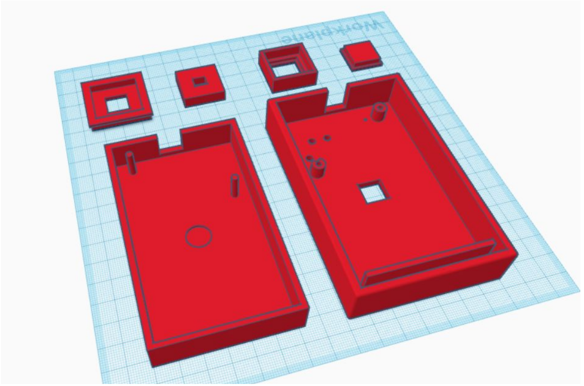


Final tested PCB (Quarter imposed for scale)

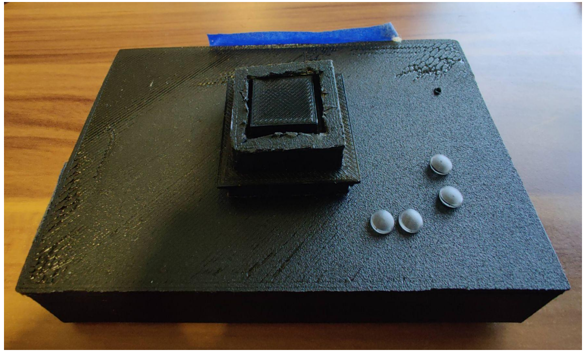
Physical Design



Circuit components designed in AutoCAD



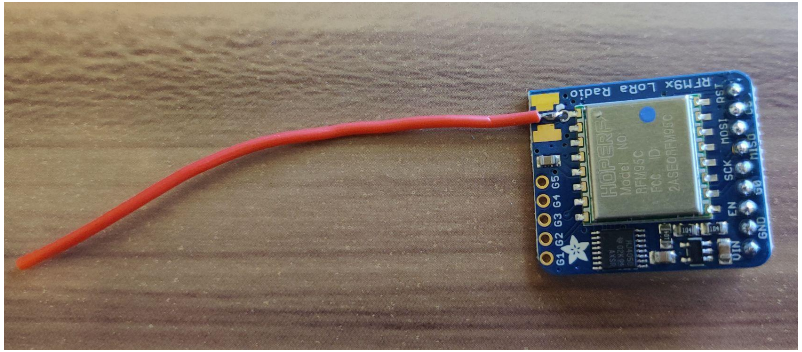
Casing prototype in TinkerCAD



Casing prototype after printing

Radio System Selection

- ➔ Primary component for transmitting / receiving data
- ➔ Why **LoRa**: **Lo**ng **Ra**nge
  - ◆ Range upto 2 km
  - ◆ Low Bitrate
- ➔ Packetized data transmission
- ➔ Transmission Frequency: 915 MHz
- ➔ Radio Unit: RFM95 LoRa Radio

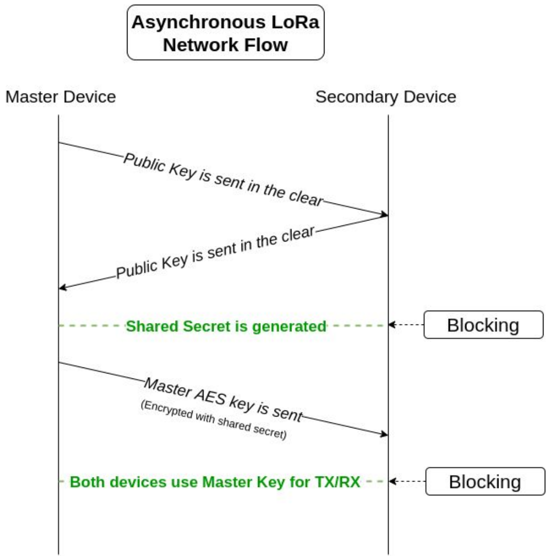


RFM9x Breakout Board with RFM95 LoRa Radio and soldered wire (monopole) antenna

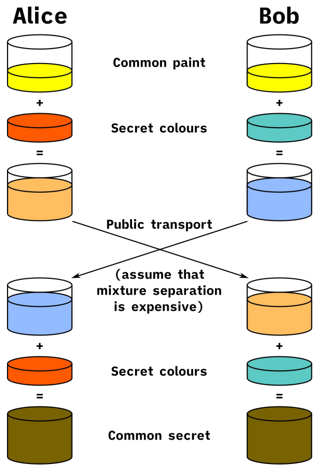
Cryptographic Design

Why is fixed secret key is not sufficient? Flexibility.

- ➔ Pairing
  - ◆ Master device <-> Secondary device
  - ◆ Diffie-Hellman key-exchange
    - *ECDH (Curve25519)*
- ➔ Standard Communication
  - ◆ Standard “password” type lock
    - *AES-128*
- ➔ Attacks considered
  - ◆ Passive man-in-the-middle
  - ◆ Replay attacks



Pairing Network Flow via LoRa radio.



Diffie-Hellman paint analogy

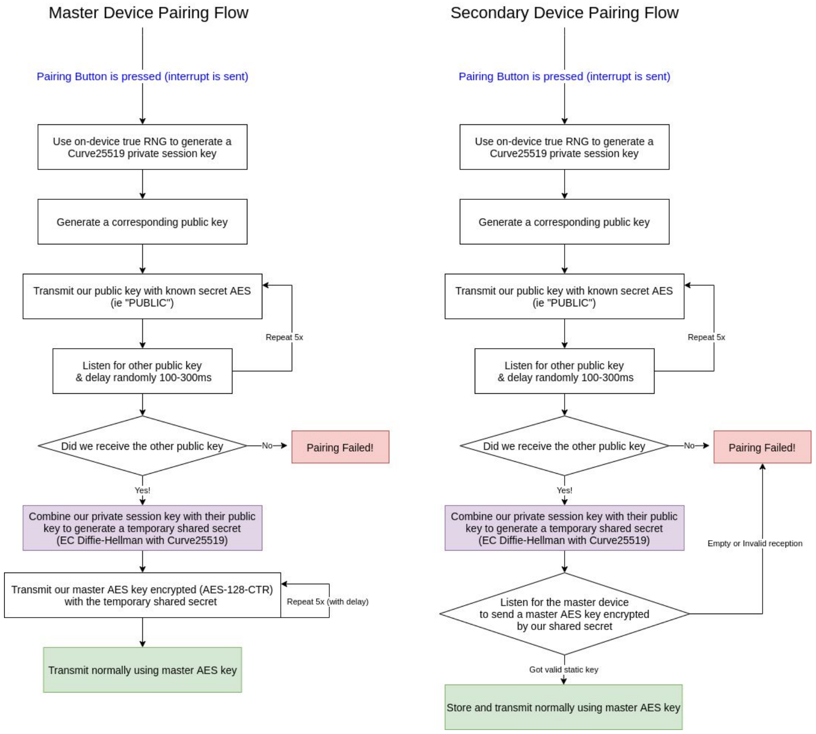
Software Design

Guiding Principles

- ➔ Robust state machine
- ➔ Strongly prefer interrupts (periodic & external)
  - ◆ Microcontroller is actually is idle most of the time!
- ➔ Lean on hardware
  - ◆ AES hardware built in
  - ◆ True random number generator (TRNG)
  - ◆ Use large flash to store secrets

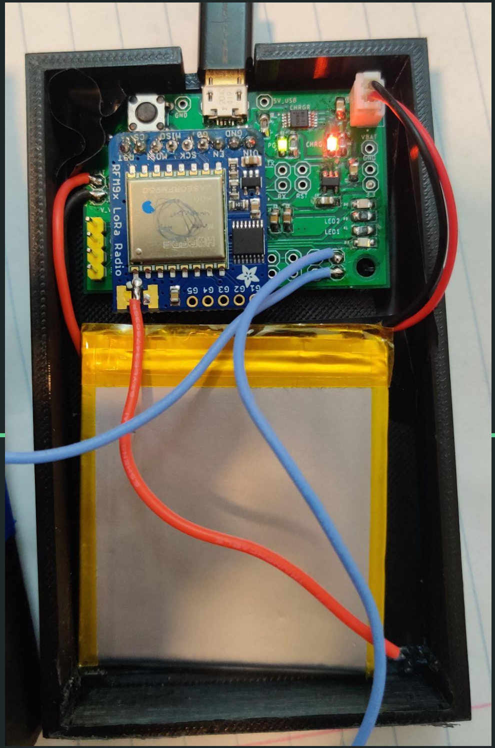
Recording Presses

- ➔ On first button interrupt, we periodically poll the button state
  - ◆ 25ms*64 samples = 1.6 seconds in each packet
- ➔ Ex:
  - ◆ `11111100000001111111111111111000000000111 ...`



State Machine for Device Pairing

Project Build



Software Implementation & Hardware Assembly

- ➔ Building a radio driver
- ➔ Radio configuration

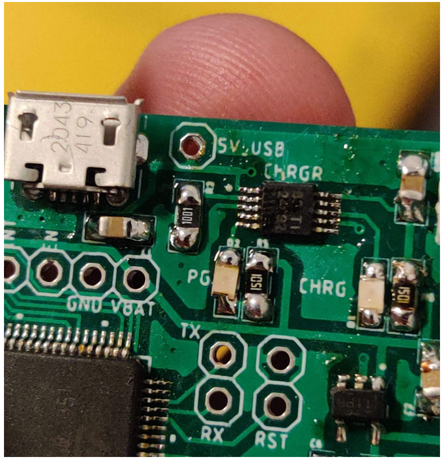
- ➔ 0.5 mm pin-pitch soldering
- ➔ LiPo charger debugging
- ➔ Debugging issues underneath radio

```
} else if (length == sizeof(Packet)) {
    Packet tmp;
    tmp.preamble = 0;
    if (HAL_CRYP_Decrypt(&hcryp, buffer, length, &tmp, 1) == HAL_OK
            && tmp.preamble == VIBE_PREAMBLE
            && tmp.sequenceNumber > deviceSeqs[tmp.deviceID]) {

        playback.data = tmp.data;
        playback.enabled = 1;
        playback.count = 0;
        deviceSeqs[tmp.deviceID] = tmp.sequenceNumber;

    }
}
```

Example snippet, interrupt based packet reception
Open source @ github.com/braeden/ece445



Close-up of charger & MCU soldering

Requirements & Verifications

Microcontroller R&V

Required Verification

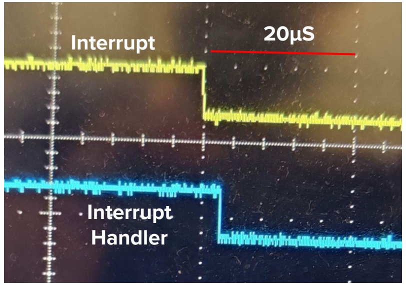
- ➔ Asymmetric encryption each <1 second
- ➔ Symmetric encryption each <10ms
- ➔ Interrupt response time <50µS

Additional Verification

- ➔ Flash read and write
- ➔ True RNG works reliably
- ➔ Periodic interrupts
- ➔ PWM is easily configurable

Operation type	Total operation time	Average time per single operation
Curve25519 Public key generation Repeated 100 times.	31.377 seconds	0.313 seconds
Curve25519 secret exchange Repeated 100 times.	31.406 seconds	0.314 seconds
AES CTR Encryption of 128 bits (1 block) Repeated 10000 times.	189 milliseconds	18.9 microseconds
AES CTR Decryption of 128 bits (1 block) Repeated 10000 times.	191 milliseconds	19.1 microseconds

Cryptographic Operation Benchmarking



Interrupt & Interrupt response (at 20µS interval)

Power System R&V

Requirement	Verification
Battery charger can handle a dead-short	Power charger & shorted pins. System shutdown until power cycle
Battery charger must provide 300mA	Charging a battery showed a current draw of ~500mA (matching config)
Regulator must supply 3.3 ±0.1V at 50mA	Placed 50 ohm load on regulator, voltage sag was negligible.

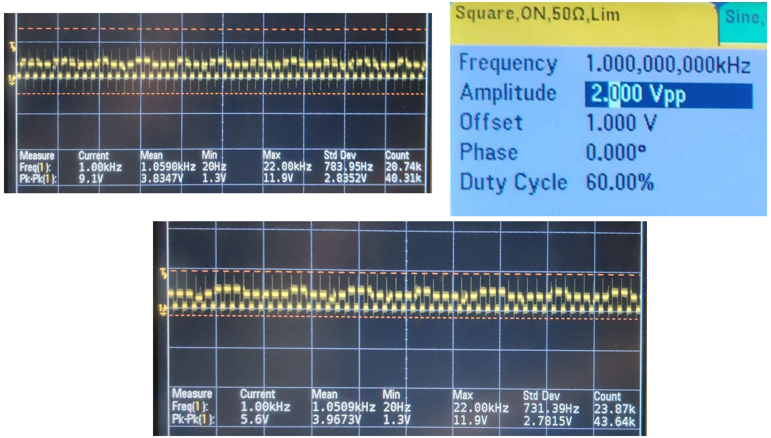
Additional Verification

- ➔ System can be independently powered by micro-USB (w/o battery)
- ➔ Estimating current draw of device to determine battery life
  - ◆ Passive
    - Device draws 22mA (experimentally)
    - 1200mAh / 22mA = **54.5 hours**
  - ◆ Active (theoretical)
    - Highest power transmission + vibration motor is at 100% duty cycle -> 200mA
    - 1200mAH / 220mA = **5.45 hours**

VS. High Level Requirements:
Passive: 54.5 vs 8 Hours!
Maximum: 5.45 vs 1 Hour!

Physical IO R&V

- ➔ Reduce back-EMF from motor
- ➔ Vibrations must be felt through case
- ➔ Vibrations should not be too loud

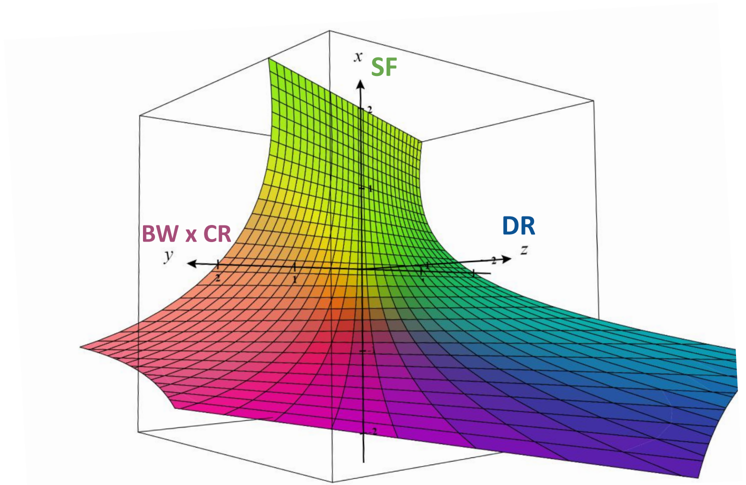


Before protection (1), signal generator (2), after protection (3). Back EMF reduced with Schottky diode & capacitor

Requirement	Verification
Prevent Back-EMF	Oscilloscope single shot capture
Vibration Level must be ideal	Decibel meter test

Radio System R&V

Item	Requirement
Transmission Range	>= 1km
Transmission Latency	<= 2s



Graph showing relationship between DR, SF, BW and CR

$$DR = SF\frac{BW}{2^{SF}}CR$$

DR = Data Rate
SF = Spreading Factor
BW = Bandwidth
CR = Chip Rate

Bandwidth BW	Spreading Factor SF	Coding Rate CR	Data Rate DR	Theoretical Latency	Actual Latency during testing
500 kHz	11	4:5	2.148 kbps	59.59 ms	~165 ms
31.25 kHz	6	4:5	2.344 kbps	54.60 ms	~42 ms
250 kHz	9	4:5	3.516 kbps	36.40 ms	~93 ms
500 kHz	6	4:5	37.500 kbps	3.41 ms	~4ms
7.8 kHz	12	4:8	11.000 kbps	11.63 ms	~23 ms

Actual transmission latencies for different values of BW, SF, CR and DR

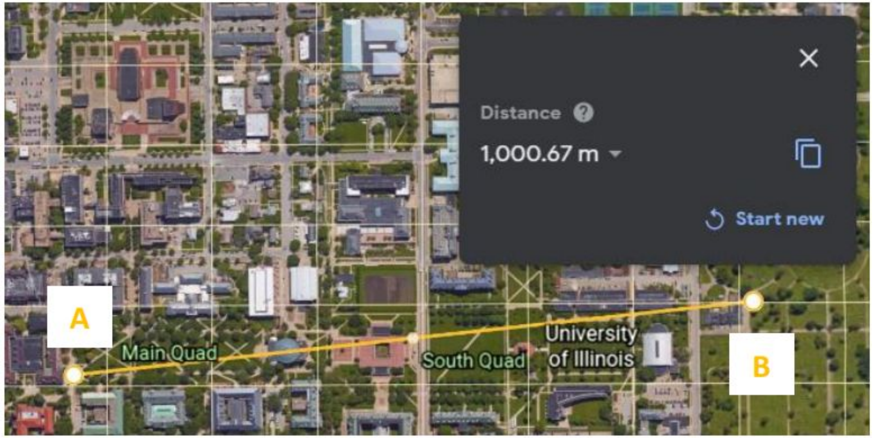
Functional Tests

Functional Tests (Hardware)

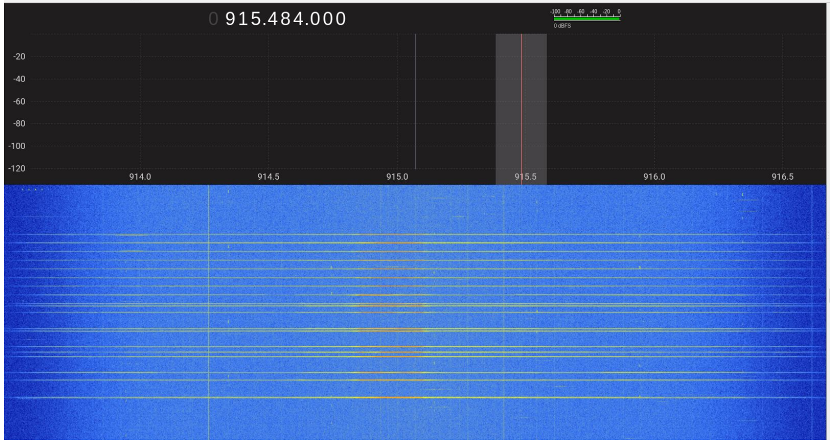
- ➔ Distance Test for Radio (>= 1km)
- ➔ Latency Test for Radio (<= 2s)
- ➔ Informal: Battery, Range

Bandwidth	:	250 kHz
Spreading Factor	:	9
Coding Rate	:	4:05
Data Rate	:	3.516 kbps
Tested Latency	:	~93 ms

Final selected Modem Configuration values for LoRa radio



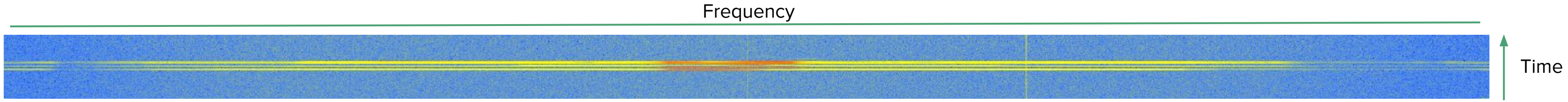
Distance test at the UofI Main Quad



Software Defined Radio (SDR) Capture of Pairing Sequence

Functional Tests (Software)

- ➔ Reliably enter/exit pairing mode & pairing works
- ➔ Radio remains in a known state
  - ◆ Sends appropriate interrupts for TX & RX
- ➔ Device rejects replayed packets (packets with the same sequence number)
- ➔ Devices are able to generate, store and recall secret keys
- ➔ Cadence of button presses is replayed on other devices
- ➔ Radio bursts N (3) packets



SDR capture: 3x duplicate packets sent in quick succession to avoid packet loss

Wrapping Up

Successes & Challenges

- Functional prototype
- Range and latency of radio
- Cryptographic standards

- 3D Printer tolerance
- Radio setup
- Software debugging
- LiPo charging configuration

Ethics

Safety & Legal:

- ➔ LiPo batteries can be a fire hazard if punctured or misused
  - ◆ Selected batteries with built-in protection circuitry
  - ◆ Charger is reputable and configured with 500mA current limit
- ➔ RF transmissions can be hazardous or illegal
  - ◆ Selected radio system that operates in license free ISM bands (915Mhz)
  - ◆ Module is FCC pre-approved for integration
- ➔ Software is built with an emphasis on security & privacy

Future Revisions

- Include:
    - On/Off switch for radio & device
    - USB configurable settings
    - Battery monitoring
- Change:
    - Antenna (internal to PCB)
    - Button
    - Vibration motor attachment
        - Current design amplifies vibrations into sound
    - Micro USB -> USB C
- Remove:
    - Mount radio module directly to PCB
    - Empty space (creating a more compact design)

Summary & Conclusions

- Project was a success!
- All requirements are completed and verified
- Minimal changes to design document
- Exploring other applications for device
  - Hospitals / Old age homes for rapid action with minimal effort
  - Can enable rapid long distance communication for hearing impaired individuals

Thank You