UKRAINIAN CATHOLIC UNIVERSITY

BACHELOR THESIS

Development of smart lock system for bicycles

Author:
Markiian ZUBRYTSKYI

Supervisor:
Oleg FARENYUK

A thesis submitted in fulfillment of the requirements
for the degree of Bachelor of Science

in the

Department of Computer Sciences
Faculty of Applied Sciences

Lviv 2020

Declaration of Authorship

I, Markiian ZUBRYTSKYI, declare that this thesis titled, “Development of smart lock system for bicycles” and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date:

"When man invented the bicycle he reached the peak of his attainments. Here was a machine of precision and balance for the convenience of man. And (unlike subsequent inventions for man's convenience) the more he used it, the fitter his body became. Here, for once, was a product of man's brain that was entirely beneficial to those who used it, and of no harm or irritation to others. Progress should have stopped when man invented the bicycle."

Elizabeth West

UKRAINIAN CATHOLIC UNIVERSITY

Faculty of Applied Sciences

Bachelor of Science

Developing smart lock system for bicycles

by Markiian ZUBRYTSKYI

Abstract

In some way all my serious projects or researches are connected to bicycles. This one is not an exception. For five years a big number of my friends' bicycles have been stolen despite the fact they used cable locks. Some of them have found their bikes by themselves, some asked police for help, some are searching till today. The goal of this work is developing of smart lock system, which uses NFC authorization before locking/unlocking cable lock. It also has alarm system, which will do a lot of noise and prevent a bike of being stolen.

Acknowledgements

I want to thank my supervisor Oleg Farenyuk for mentoring, directing during the research, for all work we have done together during my bachelor degree. I also want to thank my parents to supporting me during all this four years. A special thank to "Ride Now" cycling team members for helping during development and testing all my programming-cycling projects…

Contents

List of Figures

List of Tables

List of Abbreviations

NFC	**N**ear **F**ield **C**ommunication
RFID	**R**adio **F**requency **I**dentification
P2P	**P**eer-**t**o-**P**eer
HCE	**H**ost **C**ard **E**mulation
MCU	**M**icrocontroller **U**nit
EEPROM	**E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory
DF	**D**edicated File
EF	**E**lementary File
PIN	**P**ersonal **I**dentification **N**umber
APDU	**A**pplication **P**rotocol **D**ata **U**nit
IC	**I**ntegrated **C**ircuit
LED	**L**ight-**E**mitting **D**iode
PCB	**P**rinted **C**ircuit **B**oard
SPI	**S**erial **P**eripheral **I**nterface
I2C	**I**nter-**I**ntegrated **C**ircuit
SWD	**S**erial **W**ire **D**ebug
UART	**U**universal **A**asynchronous **R**receiver/**T**ransmitter

Dedicated to all people, whose bicycles have been stolen…

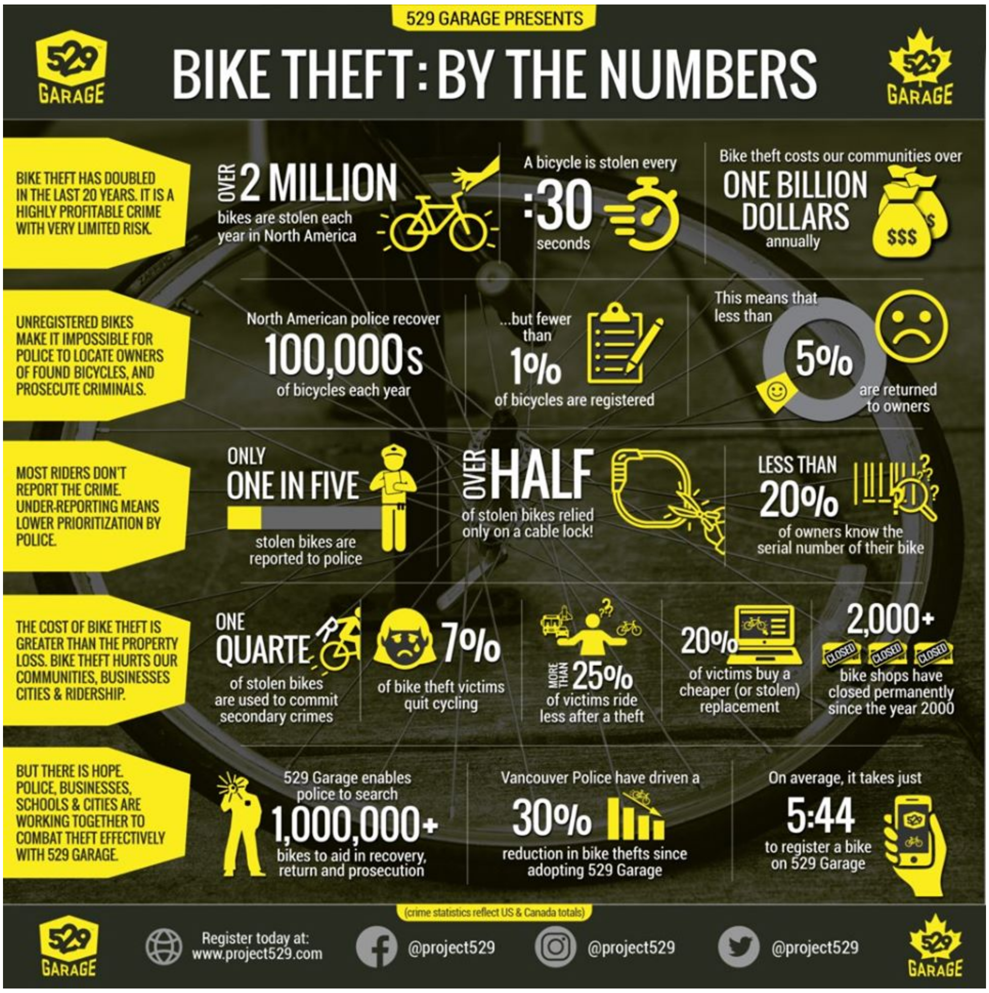
Chapter 1

Introduction

1.1 Problem

People are using bicycles in different ways all around the world today — for relaxing, traveling, as a "public transport", in professional or amateur competitions. As other things in our life, bicycles are different in usage, price and type. The price of some ones can reach even up to $10,000 – which is equivalent of a great car. One of the main disadvantages of using bicycle as private transport is the low security. According to "529 Garage" (world's biggest bike registry), only in United States over two million bikes are stolen every year [12]. Only a half of stolen bikes relied only on a cheap cable lock.

FIGURE 1.1: 529 Project Statistics


529 GARAGE PRESENTS
529 GARAGE
BIKE THEFT: BY THE NUMBERS
529 GARAGE
BIKE THEFT HAS DOUBLED IN THE LAST 20 YEARS. IT IS A HIGHLY PROFITABLE CRIME WITH VERY LIMITED RISK.
OVER 2 MILLION bikes are stolen each year in North America
A bicycle is stolen every :30 seconds
Bike theft costs our communities over ONE BILLION DOLLARS annually
$$$
UNREGISTERED BIKES MAKE IT IMPOSSIBLE FOR POLICE TO LOCATE OWNERS OF FOUND BICYCLES, AND PROSECUTE CRIMINALS.
North American police recover 100,000s of bicycles each year
...but fewer than 1% of bicycles are registered
This means that less than 5% are returned to owners
MOST RIDERS DON'T REPORT THE CRIME. UNDER-REPORTING MEANS LOWER PRIORITIZATION BY POLICE.
ONLY ONE IN FIVE stolen bikes are reported to police
OVER HALF of stolen bikes relied only on a cable lock!
LESS THAN 20% of owners know the serial number of their bike
THE COST OF BIKE THEFT IS GREATER THAN THE PROPERTY LOSS. BIKE THEFT HURTS OUR COMMUNITIES, BUSINESSES CITIES & RIDERSHIP.
ONE QUARTER of stolen bikes are used to commit secondary crimes
7% of bike theft victims quit cycling
MORE THAN 25% of victims ride less after a theft
20% of victims buy a cheaper (or stolen) replacement
2,000+ bike shops have closed permanently since the year 2000
CLOSED
CLOSED
CLOSED
BUT THERE IS HOPE. POLICE, BUSINESSES, SCHOOLS & CITIES ARE WORKING TOGETHER TO COMBAT THEFT EFFECTIVELY WITH 529 GARAGE.
529 Garage enables police to search 1,000,000+ bikes to aid in recovery, return and prosecution
Vancouver Police have driven a 30% reduction in bike thefts since adopting 529 Garage
On average, it takes just 5:44 to register a bike on 529 Garage
(crime statistics reflect US & Canada totals)
529 GARAGE
Register today at: www.project529.com
@project529
@project529
@project529
529 GARAGE

Cheap locks are made of low quality materials and can be easily broken by thieves. Using high-end materials, such as stainless steel or rubber, will increase price of the cable lock. So manufacturers decided to focus on active safe of the locks, such as alarm or GPS-trackers.

1.2 Motivation

The all "smartness" of modern smart locks is using fingerprint instead of traditional keys. The outlook of such locks are telling thieves, how to behave with a particular lock. The main idea of using Bluetooth as a key is to unlock the lock when it allows the connection to your smartphone after a long time of failed attempts. The Bluetooth's range is approximately 30 meters and this is enough for thief to steal your bike before you approach. So, the key point of this work is developing bike security system with alarm and short range NFC unlock system, which looks like common cable lock.

Chapter 2

Related works

2.1 Types of bicycle locks

When bicycles became enough popular, people started thinking about, how to protect them. Before the first bicycle lock has been invented, people had used steel chain secured by padlock. By the 1920s German and American companies produced first locks, designed for bicycles [11]. Since that time a lot of technologies have been improved and nowadays there are many different types of bicycle locks and ways to use them.

2.1.1 Cable locks

These ones are the most popular and the cheapest type of bicycle locks. Lock mechanism is already integrated. Cable is usually made from steel wire and covered with rubber. The main advantage of this type of locks is low price. Despite the fact, that wire is covered by rubber, it is easy to cut with bolt cutter. That is why this type of lock is used only in low risk area or to protect other bike components, such as wheels.

2.1.2 Chain locks

Lock mechanism is attached as combination of a chain and lock or padlock. Chain locks, which are made from low-quality materials, are easy to cut, but protection level of more expensive examples is very high and that is why they are popular among high-end bikes owners. When you use this type of lock - be ready, that your bike components will be covered with scratches for short period of time.

2.1.3 Wheel locks

The main disadvantage of this type of locks is that it locks only the rear wheel. The mechanism is mounted on the frame near rear wheel and unable its blockage. But it doesn’t prevent thief from carrying your bike on his back. So, this one is used as a secondary protection with more protective type of locks.

2.1.4 Disk rotor locks

Disk rotor locks are very similar to wheel locks. The only differ is that lock mechanism is locking front disk rotor. Like wheel locks, this type of locks should be used as secondary protection in combination with more protective lock. And of course, it cannot be used it if disk brake system is not installed on your bike.

2.1.5 U-locks

U-locks (or D-locks) are the most protective locks from all above. The lock mechanism is solid and well protected. The tube is thick (usually more than 5mm in diameter) and covered with rubber to decrease amount of scratches on a bike. The only disadvantage of U-locks is their weight - they are much heavier than other types of locks.

2.1.6 Smart Locks

Common bike locks have only passive protection - quality of materials, lock mechanism construction, size and weight. But sometimes availability of only passive protection is not enough to protect your bike from thief. Lock manufacturers started to implement different types of active protection, such as alarm, GPS tracker or key less lock system. On this way in the middle 2010s the first smart locks were produced. The main advantage is, that smart lock is actually any type of lock, but with active protection, so you can choose those types you like. But the prices of locks with high-end materials and high quality active protection are very high.

2.2 Market analysis

2.2.1 Lattis Ellipse

This U-Lock of American company was prototyped in 2014 [7]. Passive protection consists of 17mm steel U-tube and has dual-locking mechanism. The lock communicates with smartphone via Bluetooth. To lock/unlock the lock you should run app on your smartphone and manually tap proper button. This app also helps you to "share key" of your lock up to 8 friends. With help of 3-axis accelerometer Ellipse can recognize crashes and make an emergency call if you have an accident. Accelerometer is also used to recognize lock disturbance and send notifications, when it happens. Electronics is protected according to IPX4 standard. As a power source, lock uses built-in rechargeable battery, which can be charged with USB port or small solar panel. To own this lock one needs to spend about $200 .

2.2.2 I LOCK IT

Smart wheel lock from Germany [4]. Active protection system has 110dB alarm which turns on, when someone disturbs your bike. If alarm is triggered, the live tracking mode starts with help of GPS tracker. Lock/unlock process is automatic unless you enter/leave Bluetooth range. If your phone is totally discharged, you can unlock the bike with color pin. There two versions: Classic (only alarm system and Bluetooth, $100) and GPS (obviously, with GPS tracking system, $200).

2.2.3 Linka

One more wheel lock, but now from the USA [8]. It also has 110dB alarm system and 3-axis accelerometer. But body of the lock is weather proved according to IP56 standard. Built-in lithium-ion battery is a power supply and can power device up to 16 month, depending how often do you use it. It also has temperature sensor, which helps to prevent damaging the lock by freezing/overheating it. The price is $169.

2.2.4 Nocke U-Lock

One more U-lock from Utah developers [10]. One of the interesting straight among alarm system and temperature measurement is special physical key. It is strait and you can open it with custom code, which is series of long and short pushes. The price is $129.

2.2.5 Xiaomi AreoX U-Lock

Outcome of Chinese company [13]. Has dual-locking mechanism, weather resistance according to IP65 standard and fingerprint as a key. Unlocking the lock takes 0.5 second and probability of false positive is less than 0.001%. The price is $120.

Chapter 3

Background information

3.1 NFC

Near Field Communication (NFC) - set of communication protocols, which allow two electronic devices to communicate between each other over a distance up to 10 cm. It is rooted in RFID (Radio Frequency Identification) and was approved as an ISO/IEC standard in 2003. NFC device works on 13.56 MHz radio frequency and consists of reader and antenna (master) or tag and antenna (slave). Reader device generates radio frequency field, which can interact with tag or another reader device [9].

3.1.1 Modes and communication types

NFC devices can operate in three modes: Tag Reader/Writer, P2P and HCE. In first mode device can read/write information on tag or communicate with another device in this mode. In P2P mode, two devices with NFC support can interact with each other for equal data or files exchange. In HCE mode NFC device works as common NFC card/tag. There are two types of NFC communication - active and passive. Passive communication means, that there is device-initiator and device-target. Initiator generates radio frequency field, which activates device-target and makes it ready for communication. In active communication each device generates its own radio frequency field. First, device-initiator generates his own field, sends data and stops. Then device-target initialize its own field, gets information, sends request and stops.

3.1.2 NFC Tag Structure

NFC tag is passive NFC device, which has a lot of electronics under small polycarbonade body. There is no consistent power source, which is used to power memory and RF field detection unit, so energy hosting unit is used to commulate energy from external RF fields. To communicate with host MCU, communication interface is used. An EEPROM stores some data an can be configured as Read Only, Read-/Write or PIN Protected to decrease possibility of manipulation with data.

3.1.3 Data structure

The ISO7816 standart also regulates how data should be stored in NFC tags. In general, there are two types of files, which are used to build file structure: EF and DF. DF is kind of directory, which show path to EF. EF is file, which stores data. There should be at least one DF root file, which is called Mandatory File (MF), the other DF files are optional [6].

3.1.4 APDU, Applets and APDU commands

APDU is a communication interface between NFC reader and NFC tag. In fact, this is a tiny microprocessor, which can run micro programs (Applets). The main task of APDU is to receive income command and send appropriate response [5]. Both types of commands are basically byte sequences. An APDU Command consists of two parts: header (4 byte sequence) and body (up to 65 535 bytes data). APDU response also consists of two parts: data sequence and two status bytes.

CLA	1 byte	Class of command
INS	1 byte	Command instruction
P1	1 byte	Instruction parameter
P2	1 byte	Instruction parameter
Lc	0/1/3 byte/s	Data length (0 if no data, 1 byte if short APDU, 3 bytes if long APDU)
Data	Nc bytes	Data to be sent
Le	1/2/3 byte/s	Length of the response

TABLE 3.1: APDU Command structure

Data	Nc bytes	Data
SW1	1 byte	Status byte
SW2	1 byte	Status byte

TABLE 3.2: APDU Response structure

3.1.5 NDEF Messages

NDEF is standardized format of communication, which can be used by different types of NFC devices and NFC tags. Each NDEF message consists of one or multiple NDEF records. The structure of NDEF record is as follows:

TNF	3 bytes	Type Name Format, describes record type
IL	1 byte	ID Length flag, indicates ID Length field is filled or not
SR	1 byte	Indicates if length of payload is 1 byte or less
CF	1 byte	Indicator flag, which shows, if current record is first or middle one in the message (0 for first, 1 for other)
ME	1 byte	Message end flag, indicates last record of the message (is set to 1 in such case)
MB	1 byte	Message Begin flag, indicates first record of the message (is set to 1 in such case)

TABLE 3.3: Header of NDEF record (8 bytes)

Type Length	Type length in bytes
Payload Length	Payload length in bytes
ID Length	ID length in bytes
Record Type	Record type (there are 7 different types, depending on data you want to send)
ID	ID of record
Payload	Data to be sent

TABLE 3.4: Body of NDEF record

3.2 Fourier analysis

In this device accelerometer is using for vibration and movement recognition. During vibration analysis, two components of vibro-signal are taken into an account: frequency and amplitude. Analyzing frequency can show us the source of a problem or anomaly behaviour. The bigger is amplitude, the stronger is vibration and the anomaly behaviour can easily be found.

Fourier analysis (also called as Fourier Transformation) is state-of-the-art approach, which converts finite sequence of data from its original domain to a representation in the frequency domain. Fourier analysis is widely used for different problem solutions in such areas like engineering, music and science. In this particular case, Fourier Transform is used to convert changes of linear velocity into amplitude of changes. There are different implementations of Fourier Transforms and in order to decrease computation complexity, Fast Fourier Transform (next times FFT) is used.

Suppose, we have $a_0, a_1, a_2, ..., a_{n-1}$ sequence of data. FTT transforms this sequence to $b_0, b_1, b_2, ..., b_{n-1}$, such as:

$$b_i = \sum_{n=0}^{N-1} a_n \epsilon^{-\frac{2\pi}{N} ni}$$

where i is in range from 0 to $N - 1$ To decrease computation complexity, different algorithms are used, for example Cooley and Tukey's algorithm [1].

Chapter 4

Proposed approach

4.1 Architecture and functionality description

The main idea is using electronics to give user permission to insert real key. In the end of locking cylinder there is trailer, which checks, if key is inserted or not. In case of key (or a picklock) is inserted before digital permission, the program interrupts and alarm turns on. One more cause of turning on the alarm is recognizing vibration or moving device before digital permission. Vibrations or moves are recognized with accelermeter.

The main part of architecture is lock with electronics inside. NFC chip is working in Power Down Mode and waiting for external RF to be activated. To activate it and lock/unlock the lock the following action in Android app should be taken. After confirmation of the action smartphone should be placed near NFC chip. RF, which is generated by smartphone, awakes NFC module and communication starts. In success, the following response comes from lock and the action is confirmed.

4.2 Hardware

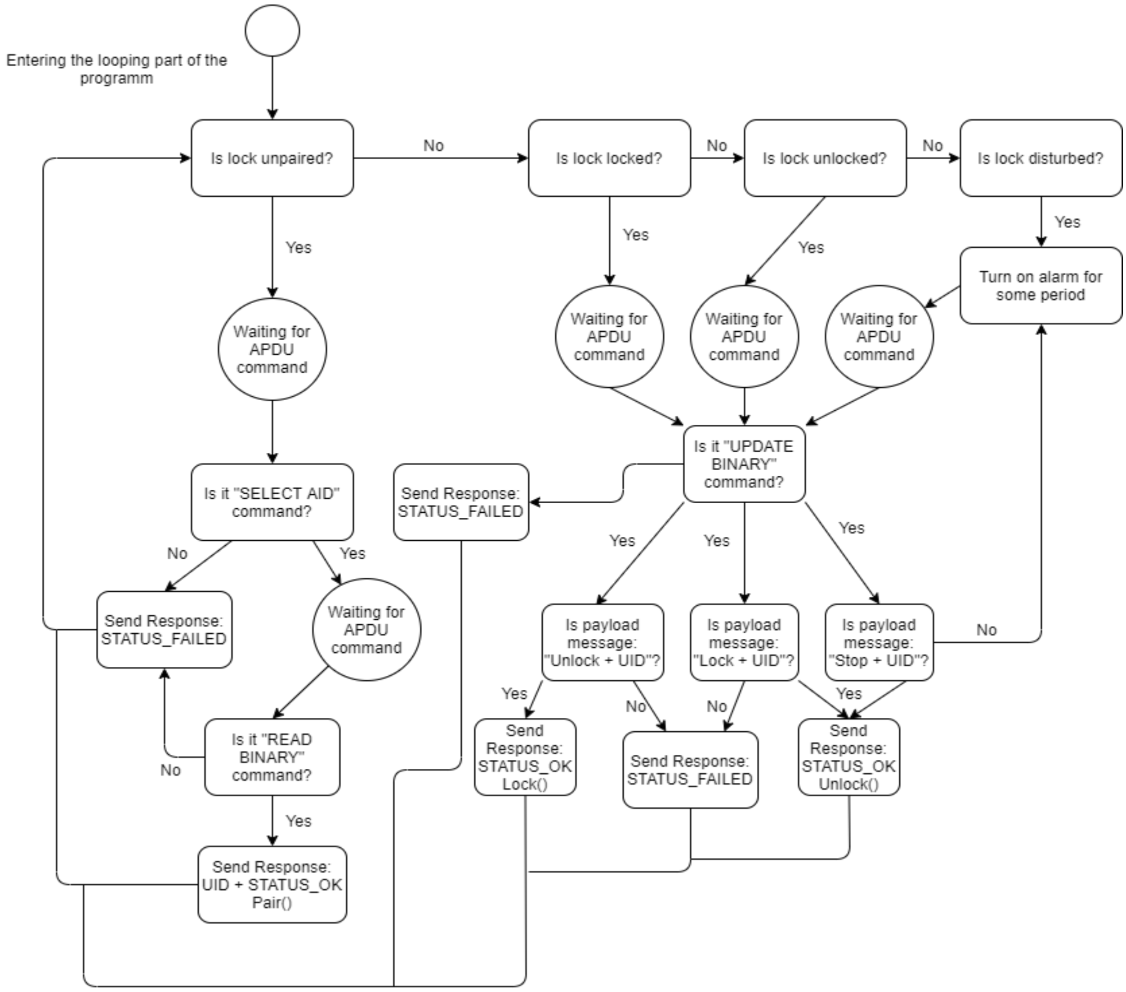
4.2.1 Components

For prototyping purpose, STM32F103C8T6 is used as MCU. It is powered from Li-ion battery with 5V and 2200mAh. In order to step down voltage to 3.3V, which is required for STM32, IC Linear Regulator RT9193-33 is used. To make battery rechargeable directly on prototype, TP4056 Li-ion charging controller is used. The battery status indicate two LEDs - red one is blinking during charging process, green one indicates stand-by mode. It can be charged via micro USB port. As the NFC module, NXP PN532 chip is connected to PCB by wires via SPI bus. To measure vibration or movement MPU6050 is used. Simple alarm system alerts a danger or attempted theft.

4.2.2 Program implementation

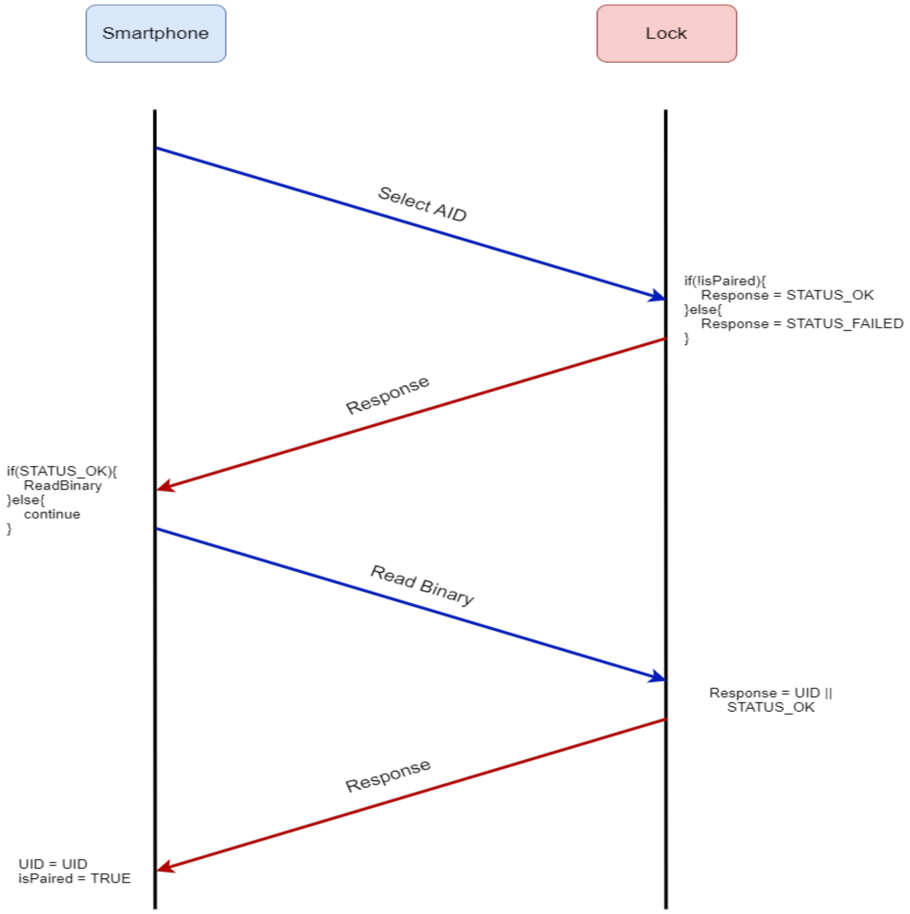
The firmware starts with initializing peripheral and setting up SPI, I2C buses in an appropriate mode. If lock was turned off (for example, has completely discharged), program loads data from flash memory. After this, PN532 NFC chip and MPU6050 sets up initial parameters. The looping part of a program is basically finite-state machine, which has two main states - PAIRED and UNPAIRED. A PAIRED state has also three sub-states: LOCKED, UNLOCKED and DISTURBED. So, finite state-machine has a following algorithm:

FIGURE 4.1: Lock/Unlock process


Entering the looping part of the programm
Is lock unpaired?
No
Is lock locked?
No
Is lock unlocked?
No
Is lock disturbed?
Yes
Yes
Yes
Yes
Turn on alarm for some period
Waiting for APDU command
Waiting for APDU command
Waiting for APDU command
Waiting for APDU command
Is it "UPDATE BINARY" command?
Is it "SELECT AID" command?
Send Response: STATUS_FAILED
No
Yes
Yes
Yes
Yes
Send Response: STATUS_FAILED
Waiting for APDU command
Is payload message: "Unlock + UID"?
Is payload message: "Lock + UID"?
Is payload message: "Stop + UID"?
No
Yes
No
No
Yes
Is it "READ BINARY" command?
No
Send Response: STATUS_OK Lock()
Send Response: STATUS_FAILED
Send Response: STATUS_OK Unlock()
Yes
Send Response: UID + STATUS_OK Pair()

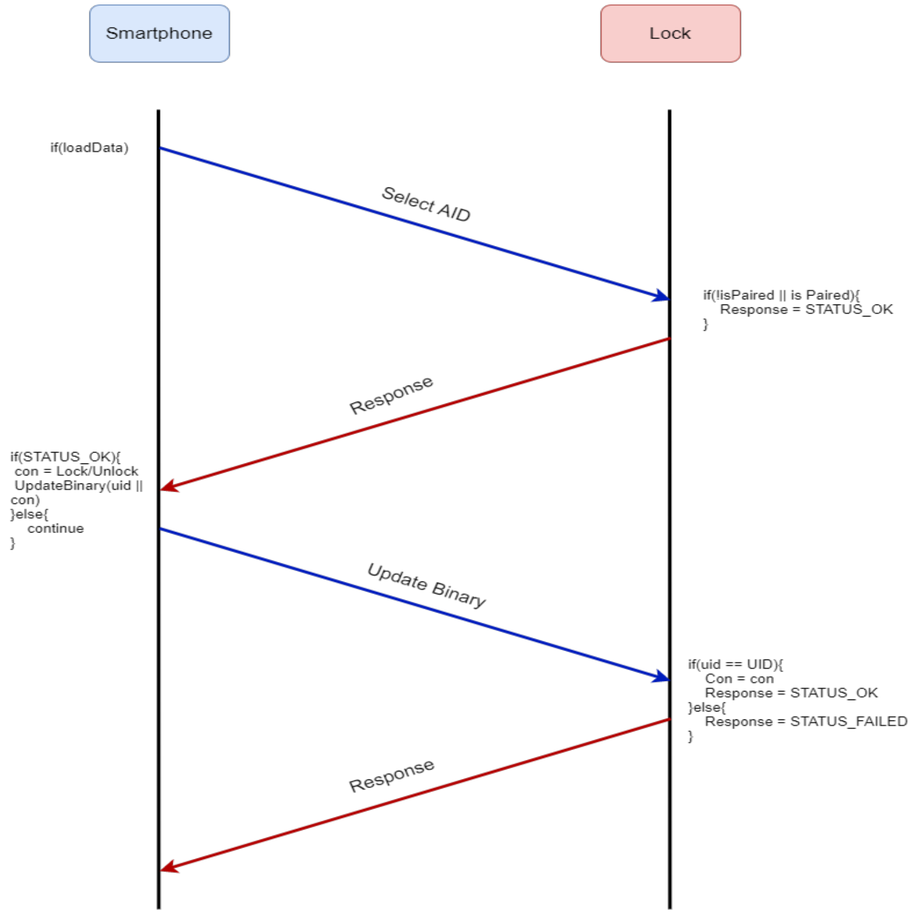
If lock is unpaired it basically waits for smartphone, which requests to create a pair. To have proper communication with smartphone, the corresponding program of APDU (Applet) should be chosen:

FIGURE 4.2: Creating a pair



After pair was created lock switches to Power Down Mode and waits for action. Lock/unlock process looks as follows:

FIGURE 4.3: Lock/Unlock process



```
if(loadData)
```

```
if(!isPaired || is Paired){
    Response = STATUS_OK
}
```

```
if(STATUS_OK){
 con = Lock/Unlock
 UpdateBinary(uid ||
con)
}else{
    continue
}
```

```
if(uid == UID){
    Con = con
    Response = STATUS_OK
}else{
    Response = STATUS_FAILED
}
```

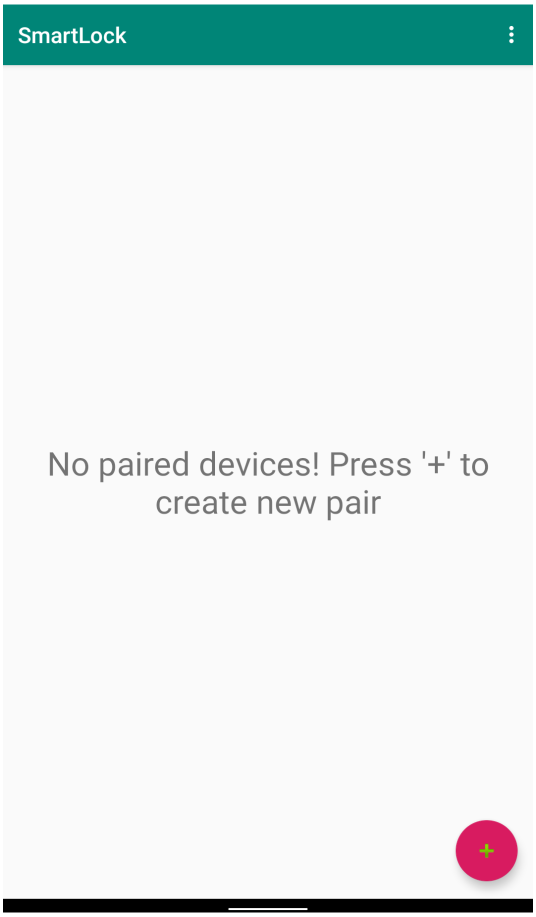
Accelerometer measures data and if anomaly behaviour occurs, a program interrupts. An interrupt function changes state to DISTURBED. In case of this state, the alarm system is turning on and working till you place the smartphone near the lock.

4.3 Android application

The main key of the lock is smartphone. So, it was decided to start with Android, because of accessibility and versatility. Using Android application, user can create new pair with a lock, lock/unlock it or turn off the alarm, when the device was disturbed by thieves and siren produces loud sound. The main point of using smartphone as a key is allowing real key insertion via NFC module. Without this permission it is unable to do something with lock even with real key.

A simple Android application was developed using Android Studio IDE. After launching app, the start menu appears:

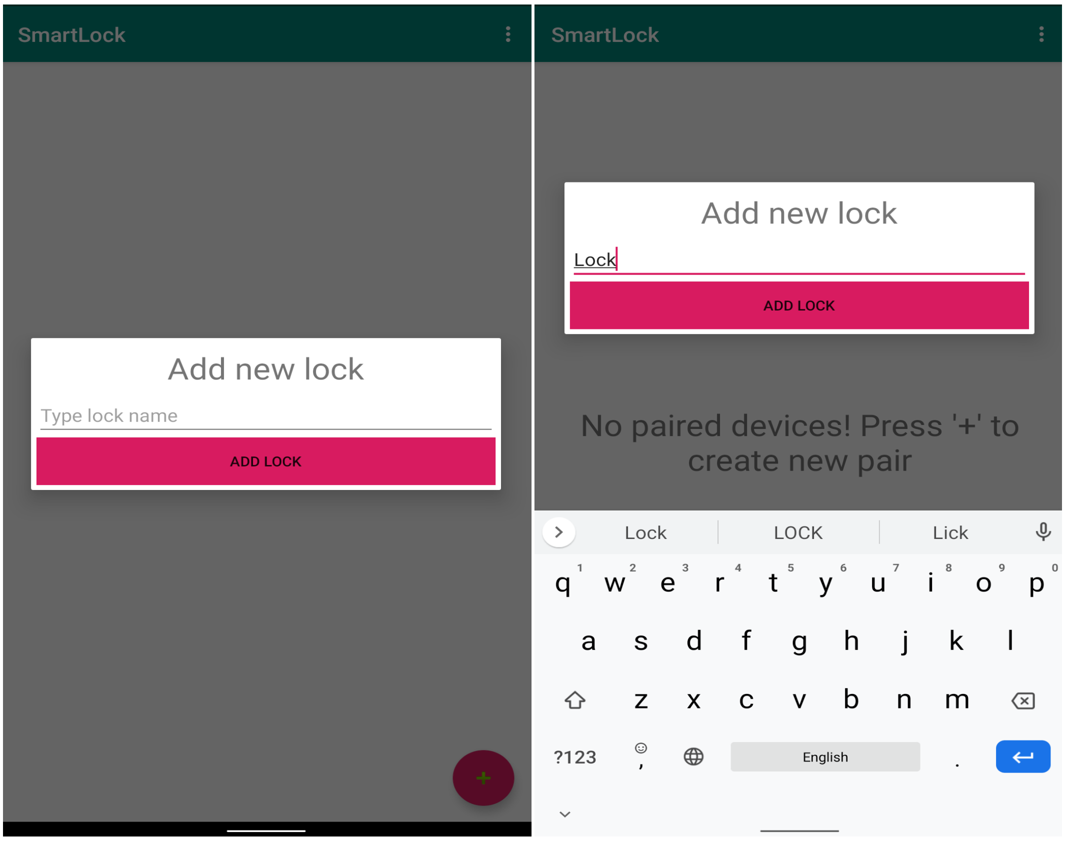
FIGURE 4.4: Start menu



No paired devices! Press '+' to create new pair

Tapping on "Add" button in right down corner of the screen, we can create a pair, adding new lock. After tapping a button, popup menu appears asking user to enter name of the lock. Having typed name and tapping on "Add Lock" button we get, as a result of this action, a popup window requesting user to place a smartphone near lock for pairing. If response from lock is STATUS_OK code - the user will see the following popup-message:

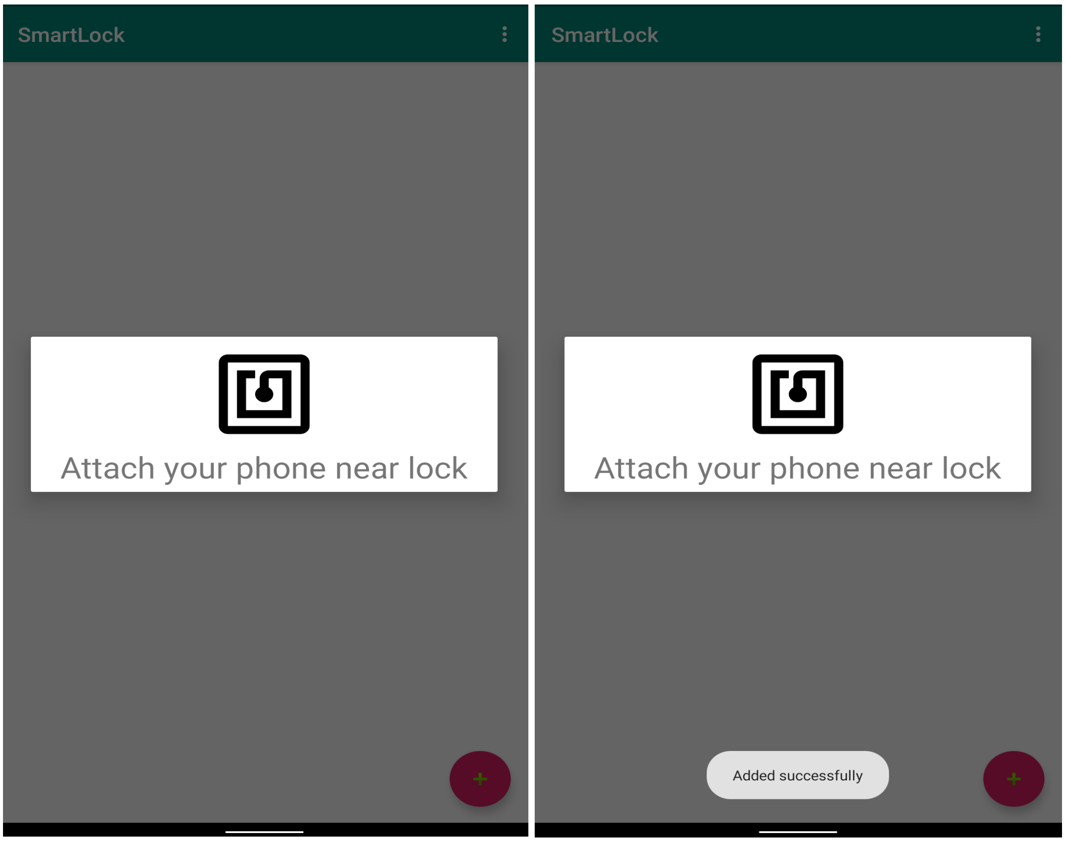
FIGURE 4.5: Add lock - (1) left, (2) right



Lock

No paired devices! Press '+' to create new pair

FIGURE 4.6: Add lock - (3) left, (4) right



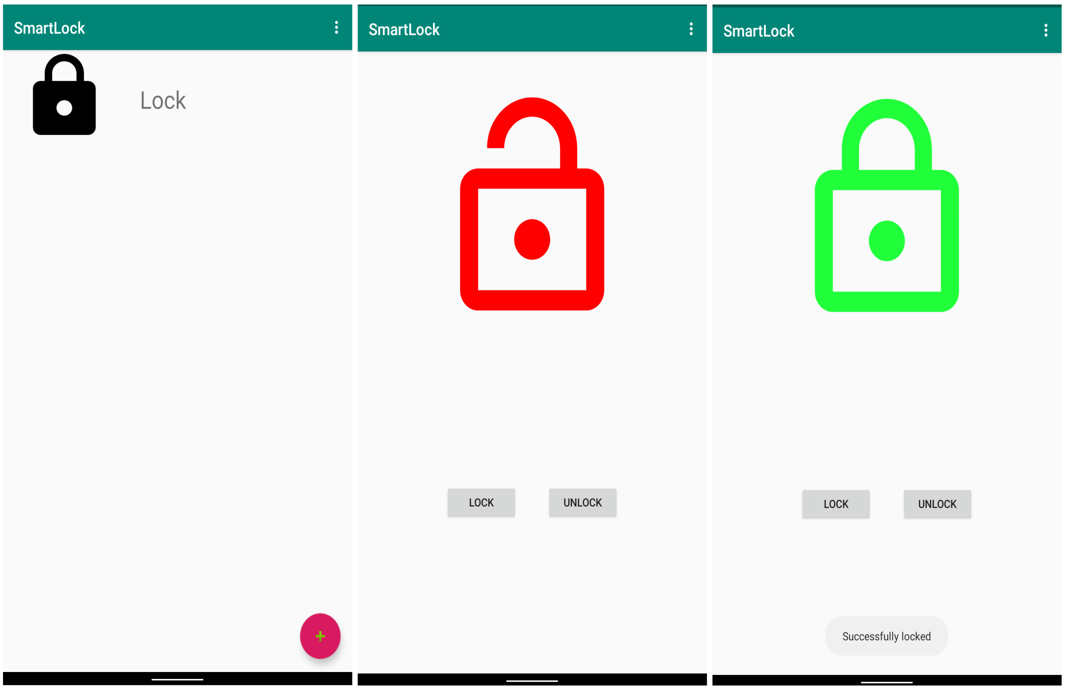
Attach your phone near lock

Attach your phone near lock

Added successfully

When user returns to start menu after lock adding process, all paired locks will be displayed there. To use proper lock, user should simply tap on lock he wants to communicate with. After choosing lock, the control window of chosen one will be displayed. There are two buttons, which allow user to lock and unlock the device. After tapping one of these buttons, smartphone asks user to put it near the lock. The following popup-window (which is the same as during creating pair process) will be displayed. If lock returns STATUS_OK code - padlock icon will change its style and color according to the state.

FIGURE 4.7: Lock control - (1) left, (2) middle, (3) right



To implement communication process with lock, "NfcMessage" [2] and "NfcRecord" [3] packages were used.

4.4 Schematic and PCB

All schematics and PCB were designed in CircuitMaker environment. As it is a prototype - there is SWD output in order to have ability to reflash firmware into MCU. 3D PCB design is also included.

FIGURE 4.8: Schematics of the prototype

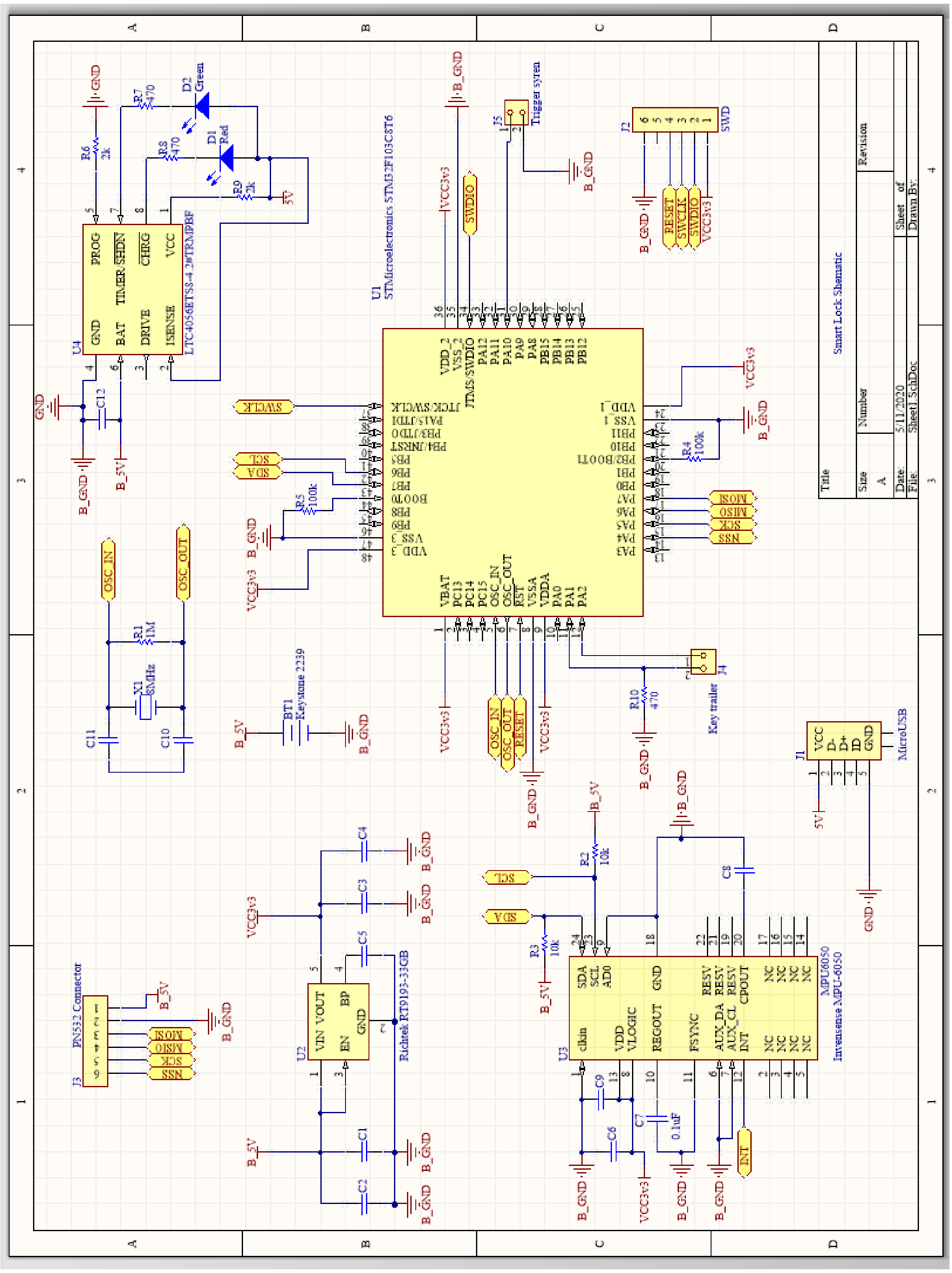
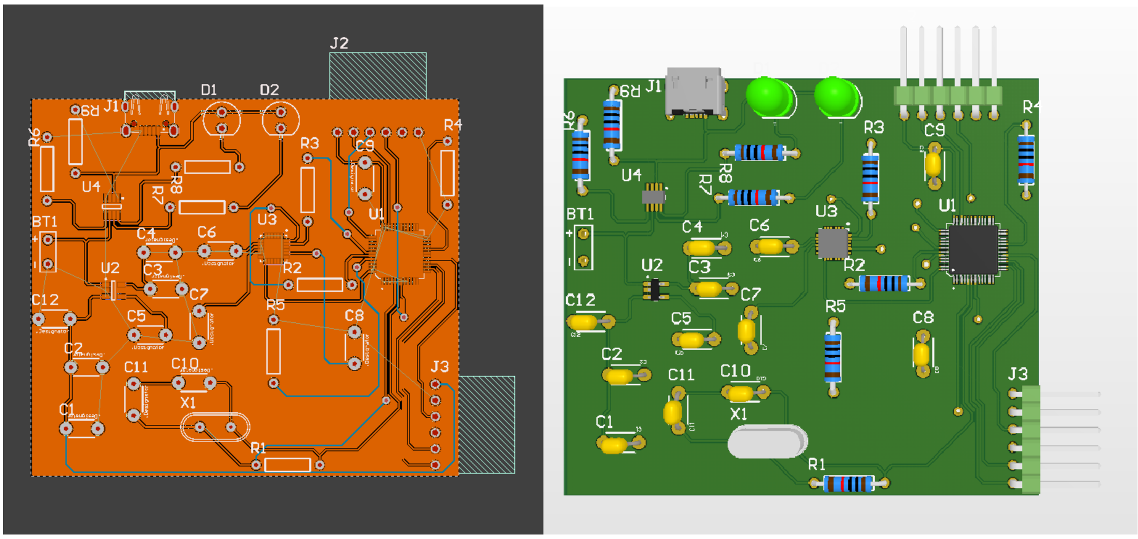


FIGURE 4.9: PCB design (left) and 3D design (right)



Chapter 5

Results and future work

5.1 Results

As a result of this work, there is a first smart lock ever, using NFC module as communication unit. The main advantages of using NFC are power savings efficiency and short working range. The last advantage reduces possibility to hack active protection of the lock. A level of passive protection will affect a cost of future product, so it should be a balance between quality and price.
During development and testing vibration recognition algorithm, the results of Fourier Transform were sent to PC via UART to build real time plots. Here, two types of graphs, which recognize the same behaviour, are attached:

FIGURE 5.1: Vibration amplitude plot (X axis only)

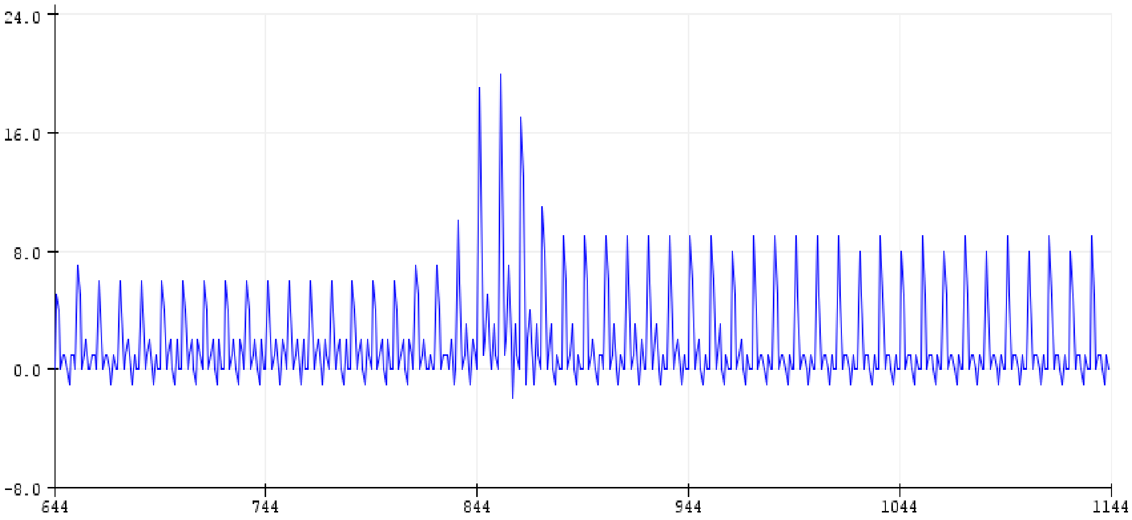
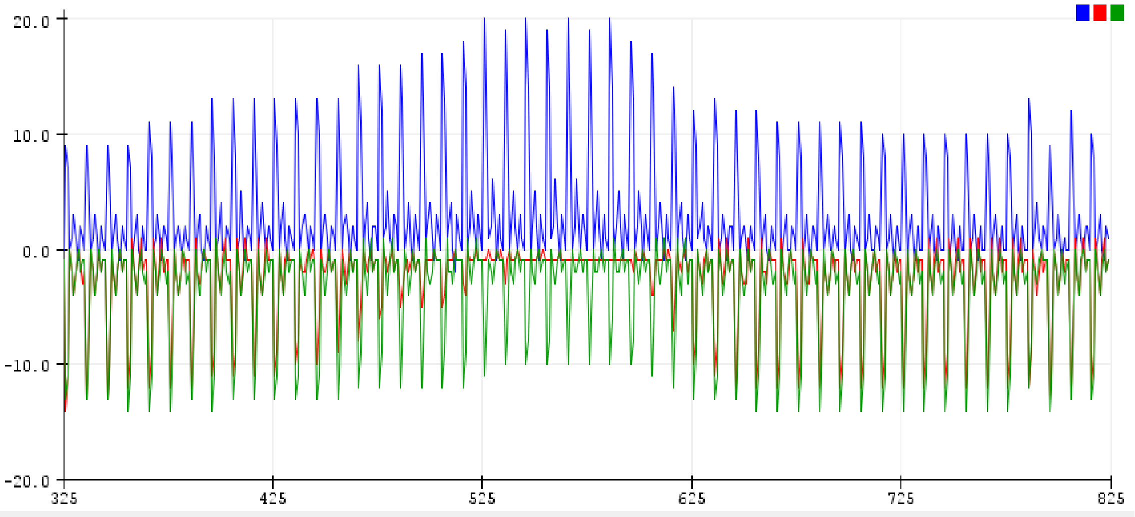


FIGURE 5.2: Vibration amplitude plot (all 3 axis)



5.2 Future work

The next step for improving prototype is mostly connected to Android application. Such options as key sharing, several paired locks support sound like great plan. One more thing to work with hardware is adding possibility to open lock without smartphone, only using a real key. It can be implemented in following way: the first insertion of key should take a proper amount of time (can be set in Settings) - it indicates emergency situation. Then, using combination of different types of insertion time as a PIN (can also be set in Settings), the lock can be locked/unlocked.

Bibliography

[1] *An Algorithm for the Machine Calculation of Complex Fourier Series*. 1965. URL: https://www.ams.org/journals/mcom/1965-19-090/S0025-5718-1965-0178586-1/S0025-5718-1965-0178586-1.pdf.

[2] *Android Developers Documentation - NDEF Message*. URL: https://developer.android.com/reference/android/nfc/NdefMessage.

[3] *Android Developers Documentation - NDEF Record*. URL: https://developer.android.com/reference/android/nfc/NdefRecord.

[4] *I LOCK IT description and specifications*. URL: https://ilockit.bike/produkt-kategorie/locks/.

[5] *ISO 7816-4 section 6 - Basic Interindustry Commands*. URL: https://cardwerk.com/smart-card-standard-iso7816-4-section-6-basic-interindustry-commands/.

[6] *ISO 7816-4 standard*. URL: https://cardwerk.com/iso-7816-part-4/.

[7] *Lattis Ellipse description and specifications*. URL: https://lattis.io/products/ellipse.

[8] *Linka description and specifications*. URL: https://www.linkalock.com.

[9] *NFC Forum*. URL: https://nfc-forum.org/our-work/specification-releases/specifications/.

[10] *Noke U-Lock description and specifications*. URL: https://noke.com/u-lock.

[11] Clemitson S. *A History of Cycling in 100 Objects*. Bloomsbury, 2017.

[12] D. S. Williams. *Project 529*. URL: https://project529.com/garage.

[13] *Xiaomi AreoX description and specifications*. URL: https://xiaomi-mi.com/appliances/areox-u8-smart-fingerprint-u-lock-long/.