Schnorr Protocol Fob
ECE 445 Design Document Fall 2024

Michael Gamota, Vasav Nair, Pedro Ocampo
Professor: Cunjiang Yu
TA: Pusong Li

Table of Contents

Introduction

Problem

Current car fobs and garage door fobs are susceptible to different types of attacks. One common method for code generation includes the use of a counter, meaning both devices have an agreed upon “next code”, however this makes them susceptible to rolling jam attacks. This attack involves a malicious third party intercepting(jam and store) a valid unlock/open signal sent by a button fob. When the user tries to unlock the device again, the signal is again intercepted, but the third party sends the first intercepted code to the receiver. Now, the third party has the next valid code. Garage doors may use either a fixed code or have a counter based code, which makes them susceptible to replay attacks or rolling jam attacks, respectively.

Cars with passive fobs can be stolen using relay attacks. Passive fobs require the presence of a scanner, which emits EM radiation to power the passive fob which returns a code wirelessly. With a passive fob, a malicious actor just needs to artificially extend the reader(located on the exterior of a car) to trigger a response from the passive fob.

Therefore, all of these fob technologies have vulnerabilities which are relatively easily exploitable. We find this to be unreasonable as access to one’s house or car is something that should be protected with the highest level of security.

Solution

Our solution is to design the hardware for a key fob(prover) and verification and control(verifier) unit which will leverage Schnorr protocol, an authentication scheme which uses public key encryption to implement an interactive zero-knowledge proof. What this means is that, first, the fob(prover) will have a public key and private key, which can be thought of as a known serial number, and an associated secret serial number. Second, there will be an interaction between the key fob and the verification and control unit, the fob will send a message to the lock/opener, announcing its public key and the desired command. The lock/opener will respond with a “challenge”, which is a random number. The key fob will then compute the response to the “challenge” which requires knowledge of the secret key. This response is sent back to the lock/opener which can then mathematically verify if the fob has disclosed its true public key in the first message. If the public key is verified as honest and it is on a preprogrammed list, the verification and control unit will unlock the car/open the garage door. The last element of Schnorr protocol is that it is a zero-knowledge authentication scheme, which means that no information about the secret key can be gained by a third party listening in or the verification and control unit.

For the purposes of our final demonstration, the verification and control unit will be connected to a small motor which will spin when a valid exchange occurs.

Visual Aid

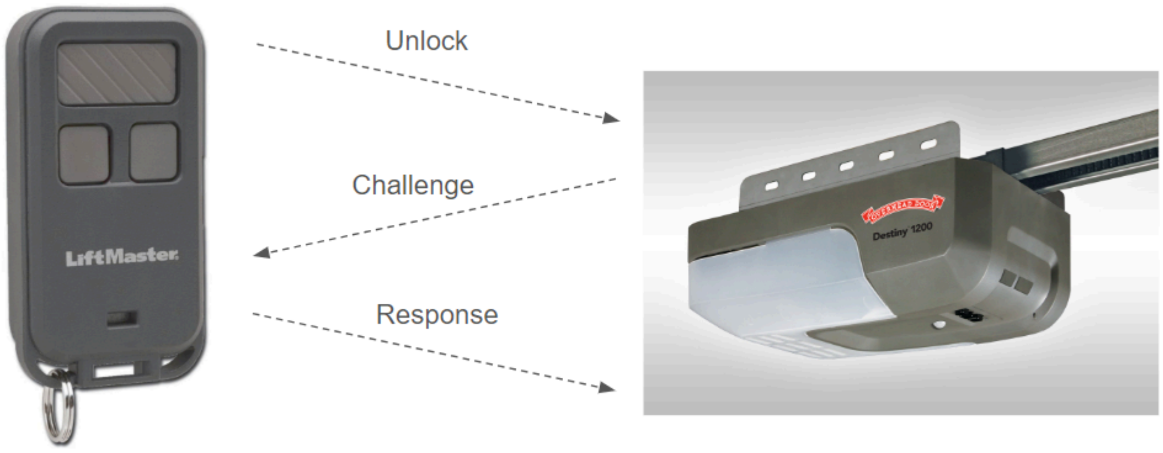


Figure 1 is an example of how our project would work at a high level

High Level Requirements

- The signals must be detected and received from 3 meters and the signal integrity must be good enough that messages are able to be authenticated.
- The time between the unlock signal being sent and the motor spinning must be less than 2 seconds.
- A replay attack is not successful

Design

Block Diagram

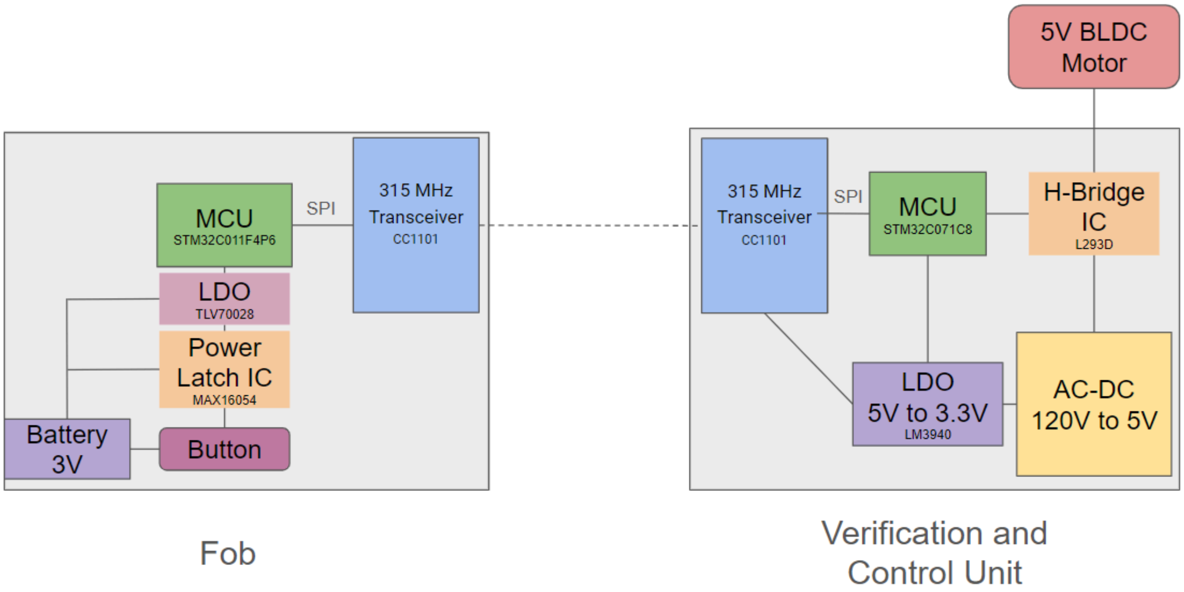


Figure 2 shows what our main components and subsystems will look like in our project, with the two main systems being the Fob and Verification & Control Unit

Physical Design

Our key fob will have a 3D printed enclosure which will make it more durable and portable. It should be small enough to fit in someone's pocket easily, so the size of a credit card is a good benchmark for this, 90 mm x 55 mm x 5 mm. The vertical dimension (5 mm) is limited by the size of the 315 MHz antenna that we plan to use.

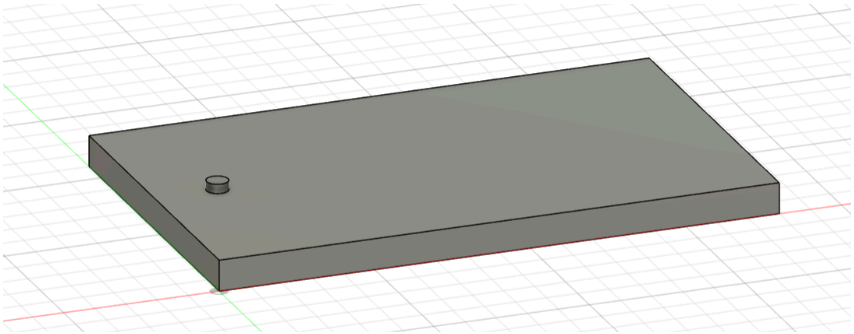


Figure 3 is a CAD Rendering of basic enclosure shape. The small bump is the button which will protrude from the enclosure

RF Transceiver and RF Chain

Identical RF transceiver subsystems are present on both the fob board and the verification and control unit. The RF transceiver communicates with the microcontroller via a SPI interface, on which the RF transceiver is the only slave device. Full-duplex (simultaneous two-way communication possible) SPI requires 4 connections between the master, the STM32 MCU [4], and the slave, the C1101 RF transceiver [5]. These 4 connections are a clock signal (SPI_SCLK), a serial communication channel from the MCU to transceiver (SPI_MOSI), a serial communication channel from the transceiver to MCU (SPI_MISO), and a slave select line (SPI_NSS). The transceiver subsystem has a few peripheral components which are required for proper functionality, which we define as wireless communication between the fob and verification and control unit at a distance of at least 3 m.

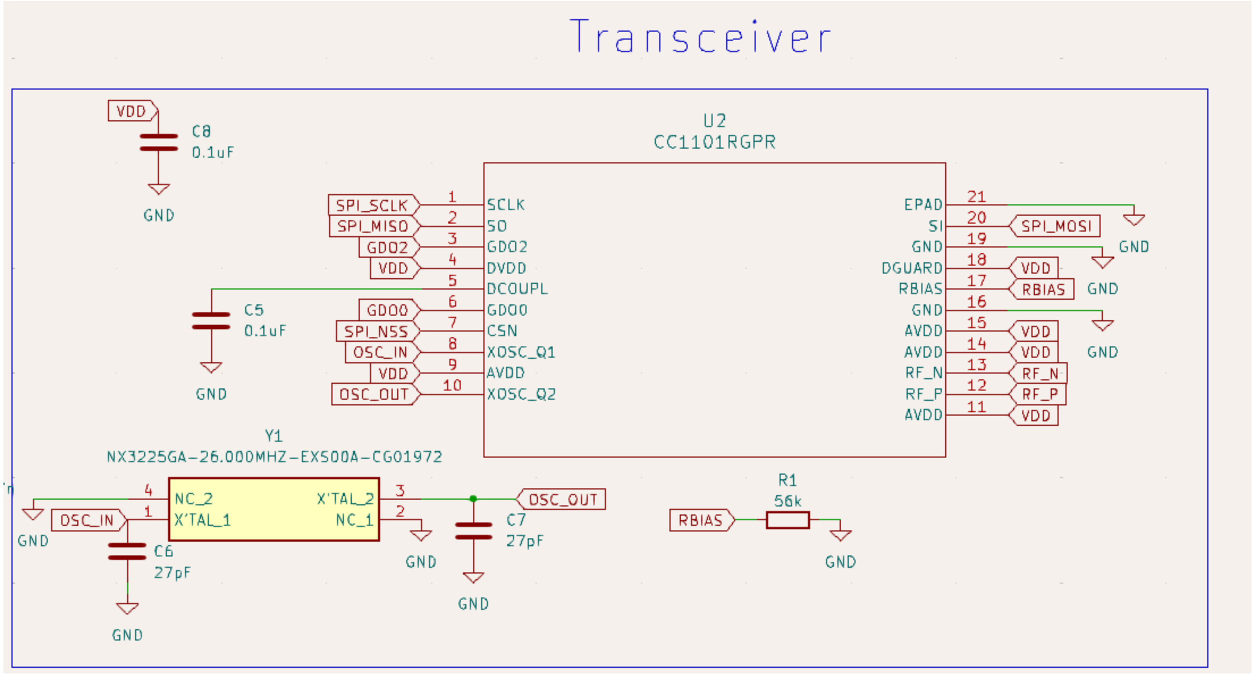


Figure 4 shows the Transceiver Circuit Schematic made within KiCad

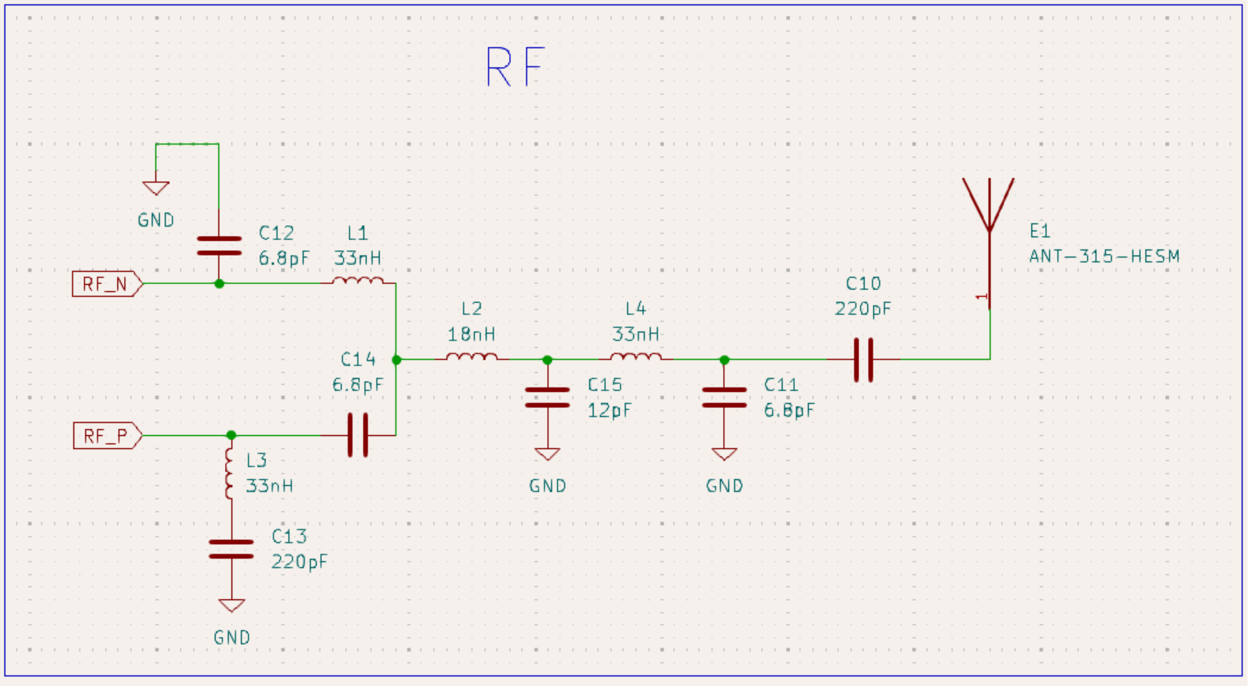
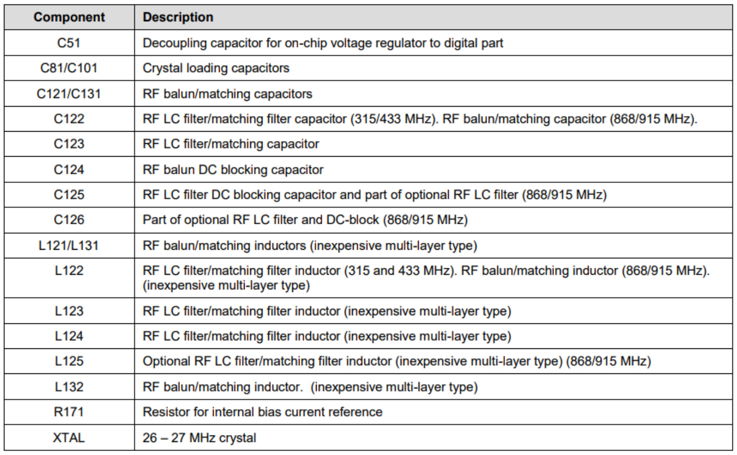


Figure 5 shows the RF chain Circuit Schematic made within KiCad



Component	Description
C51	Decoupling capacitor for on-chip voltage regulator to digital part
C81/C101	Crystal loading capacitors
C121/C131	RF balun/matching capacitors
C122	RF LC filter/matching filter capacitor (315/433 MHz). RF balun/matching capacitor (868/915 MHz).
C123	RF LC filter/matching capacitor
C124	RF balun DC blocking capacitor
C125	RF LC filter DC blocking capacitor and part of optional RF LC filter (868/915 MHz)
C126	Part of optional RF LC filter and DC-block (868/915 MHz)
L121/L131	RF balun/matching inductors (inexpensive multi-layer type)
L122	RF LC filter/matching filter inductor (315 and 433 MHz). RF balun/matching inductor (868/915 MHz). (inexpensive multi-layer type)
L123	RF LC filter/matching filter inductor (inexpensive multi-layer type)
L124	RF LC filter/matching filter inductor (inexpensive multi-layer type)
L125	Optional RF LC filter/matching filter inductor (inexpensive multi-layer type) (868/915 MHz)
L132	RF balun/matching inductor. (inexpensive multi-layer type)
R171	Resistor for internal bias current reference
XTAL	26 – 27 MHz crystal

Figure 6 shows the Component list for transceiver/RF chain

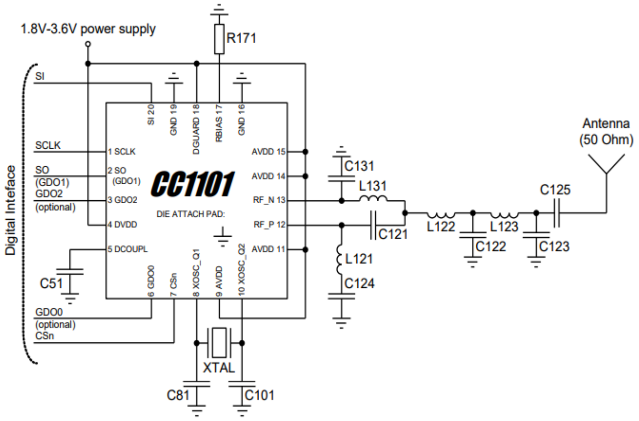
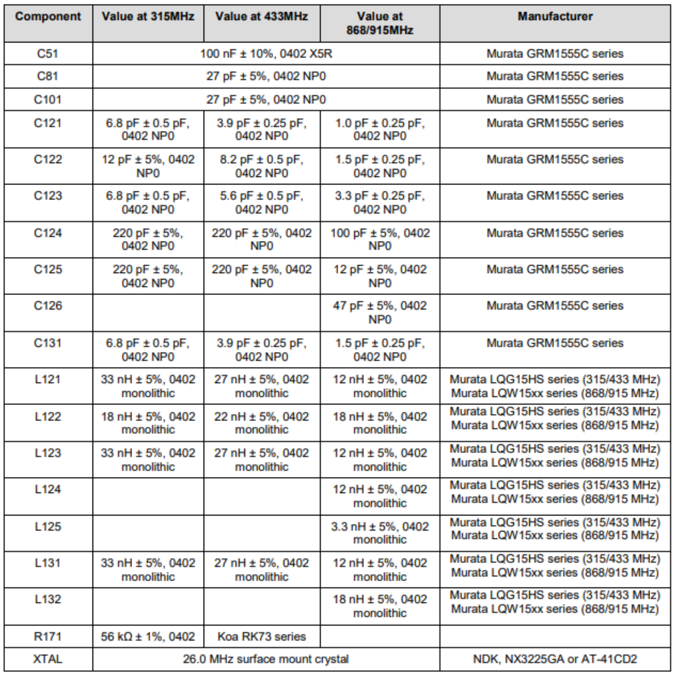


Figure 7 shows the Typical Application and Evaluation Circuit using a frequency of 315/433 MHz, excluding supply and decoupling capacitors [5].



Component	Value at 315MHz	Value at 433MHz	Value at 868/915MHz	Manufacturer
C51	100 nF ± 10%, 0402 X5R			Murata GRM1555C series
C81	27 pF ± 5%, 0402 NP0			Murata GRM1555C series
C101	27 pF ± 5%, 0402 NP0			Murata GRM1555C series
C121	6.8 pF ± 0.5 pF, 0402 NP0	3.9 pF ± 0.25 pF, 0402 NP0	1.0 pF ± 0.25 pF, 0402 NP0	Murata GRM1555C series
C122	12 pF ± 5%, 0402 NP0	8.2 pF ± 0.5 pF, 0402 NP0	1.5 pF ± 0.25 pF, 0402 NP0	Murata GRM1555C series
C123	6.8 pF ± 0.5 pF, 0402 NP0	5.6 pF ± 0.5 pF, 0402 NP0	3.3 pF ± 0.25 pF, 0402 NP0	Murata GRM1555C series
C124	220 pF ± 5%, 0402 NP0	220 pF ± 5%, 0402 NP0	100 pF ± 5%, 0402 NP0	Murata GRM1555C series
C125	220 pF ± 5%, 0402 NP0	220 pF ± 5%, 0402 NP0	12 pF ± 5%, 0402 NP0	Murata GRM1555C series
C126			47 pF ± 5%, 0402 NP0	Murata GRM1555C series
C131	6.8 pF ± 0.5 pF, 0402 NP0	3.9 pF ± 0.25 pF, 0402 NP0	1.5 pF ± 0.25 pF, 0402 NP0	Murata GRM1555C series
L121	33 nH ± 5%, 0402 monolithic	27 nH ± 5%, 0402 monolithic	12 nH ± 5%, 0402 monolithic	Murata LQG15HS series (315/433 MHz) Murata LQW15xx series (868/915 MHz)
L122	18 nH ± 5%, 0402 monolithic	22 nH ± 5%, 0402 monolithic	18 nH ± 5%, 0402 monolithic	Murata LQG15HS series (315/433 MHz) Murata LQW15xx series (868/915 MHz)
L123	33 nH ± 5%, 0402 monolithic	27 nH ± 5%, 0402 monolithic	12 nH ± 5%, 0402 monolithic	Murata LQG15HS series (315/433 MHz) Murata LQW15xx series (868/915 MHz)
L124			12 nH ± 5%, 0402 monolithic	Murata LQG15HS series (315/433 MHz) Murata LQW15xx series (868/915 MHz)
L125			3.3 nH ± 5%, 0402 monolithic	Murata LQG15HS series (315/433 MHz) Murata LQW15xx series (868/915 MHz)
L131	33 nH ± 5%, 0402 monolithic	27 nH ± 5%, 0402 monolithic	12 nH ± 5%, 0402 monolithic	Murata LQG15HS series (315/433 MHz) Murata LQW15xx series (868/915 MHz)
L132			18 nH ± 5%, 0402 monolithic	Murata LQG15HS series (315/433 MHz) Murata LQW15xx series (868/915 MHz)
R171	56 kΩ ± 1%, 0402	Koa RK73 series		
XTAL	26.0 MHz surface mount crystal			NDK, NX3225GA or AT-41CD2

Figure 8 Component list for the transceiver/RF chain

RF Transceiver/RF Chain R&V Table

Requirements	Verification
Communication from at least 3m	Program one of the 2 boards to send a basic 1 byte message. Program the other board to be in constant receive mode. Print the received message over a UART-USB converter on a laptop. Repeat in other direction
Signal integrity from at least 3m	Set a 256 bit message to be sent from one board to the other, monitor the received message by the other board by printing it to the UART interface. Verify that the received message matches the transmitted message. Verify that this works in an open space as well as with a door/wall between to simulate a garage door being opened from the outside. Repeat this process with communication in the other direction.

Fob Power System

One of the largest bottlenecks when designing mobile devices is power. Thus, one of our most important subsystems is the power tree for our fob. The power subsystem consists of a 3V coin cell battery, a MAX16054 on/off controller IC [2] which will allow us to detect the noisy signal from the push button, power up the LDO [3] , MCU, transceiver, and begin the Schnorr identification protocol. 3V was chosen because it is the most common voltage for coin cell batteries and our MCU and RF transceiver can be powered by as little as 2V and 1.8V, respectively. We are using a push button as the input to the MAC16054 [2] (per the typical application circuit). The MAX16054 [2] output is connected to the enable pin on the 2.8V LDO [3] which powers the MCU and the transceiver. This topology is used because it will limit our quiescent current draw to the sum of the quiescent currents of the MAX16054 [2] and the LDO [3].

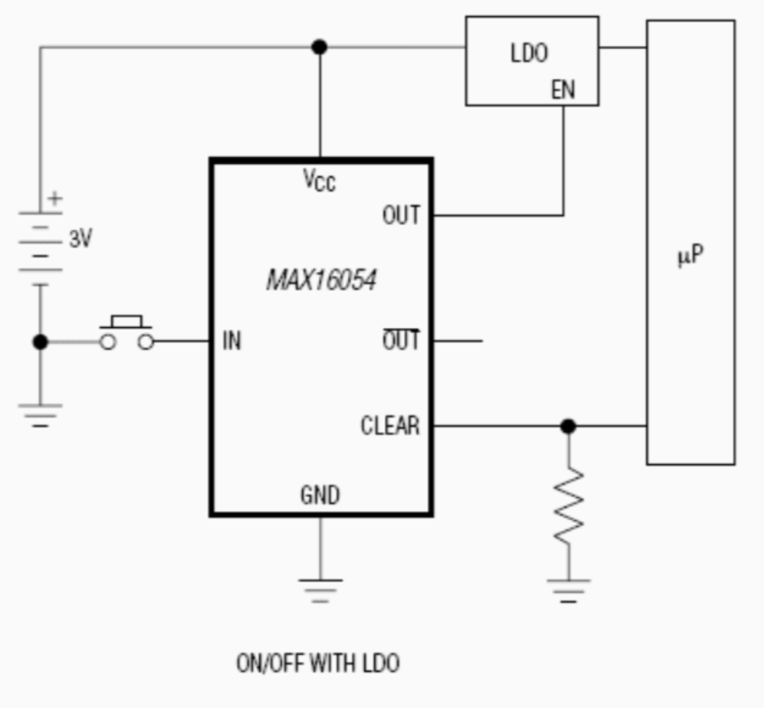


Figure 9 shows typical application circuit for MAX16054 [2]

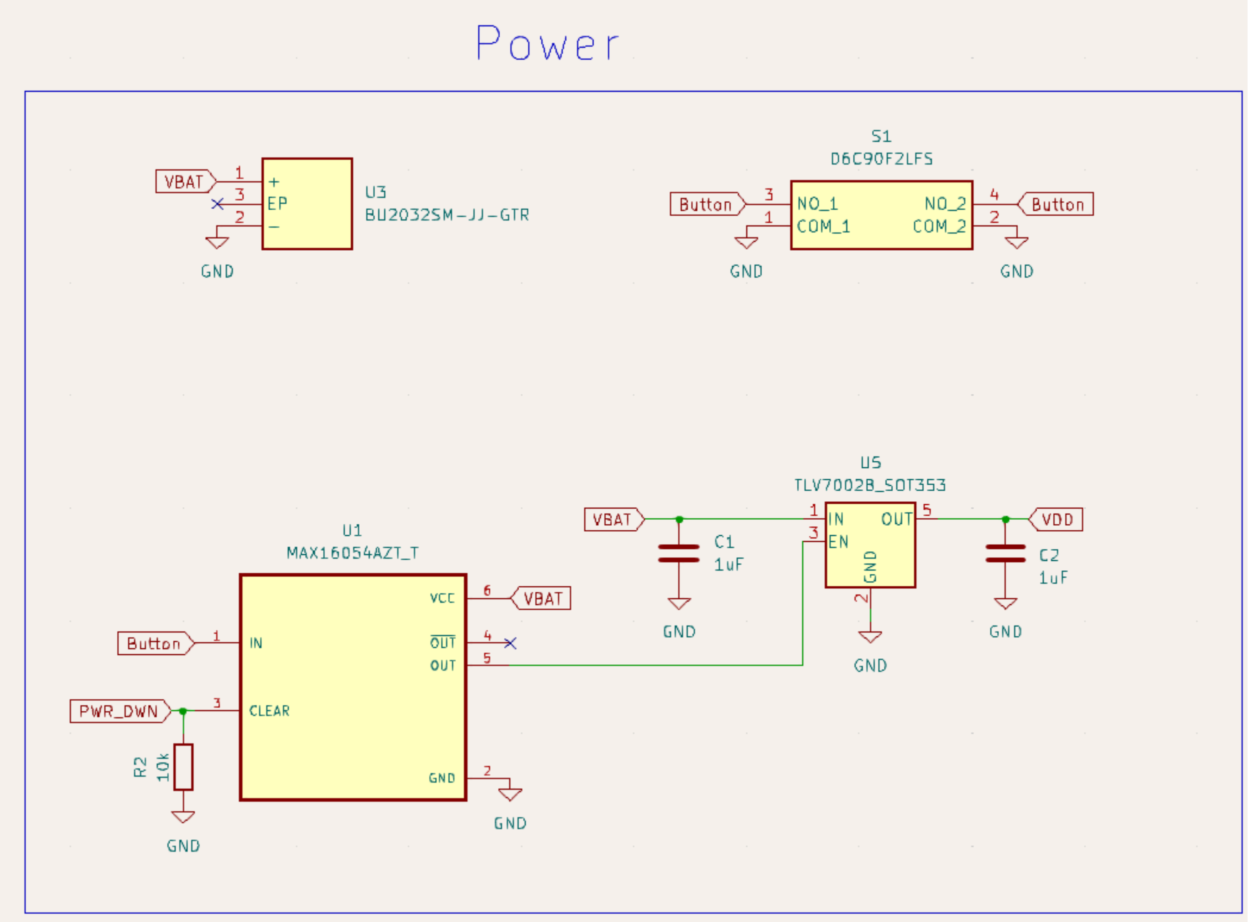


Figure 10 shows circuit schematic for power subsystem made within KiCad

Power R&V Table

Requirements	**Verification**
Power down with on/off controller works correctly	Press the button while probing the LDO output, verify that after the CLEAR pin goes high on the MAX16054, we see the LDO output disabled (<0.001 V).
Reverse voltage protection	Verify that it is impossible to insert a battery the wrong way into our holder, or if it can be jammed in, there is no output that reaches the MAX16054.
Over voltage protection	Make sure there does not exist a coin cell battery that is commonly available with over 5.5V, as this is the lower of the voltage maximums for the MAX16054 and the TLV70028 2.8V LDO

Fob MCU

We will be leveraging the SPI functionality and a few GPIOs. As explained in greater detail in the RF transceiver section, we will use a full-duplex SPI interface to communicate between the MCU and the RF transceiver. There are also a few output pins on the transceiver which can be programmed as indicator pins which may be useful in debugging, so we are also reserving GPIO pins to be used as inputs on the MCU. One GPIO pin will be configured as an output which will send the power down signal to the latch when a transaction has been completed between the fob and the verification and control unit.

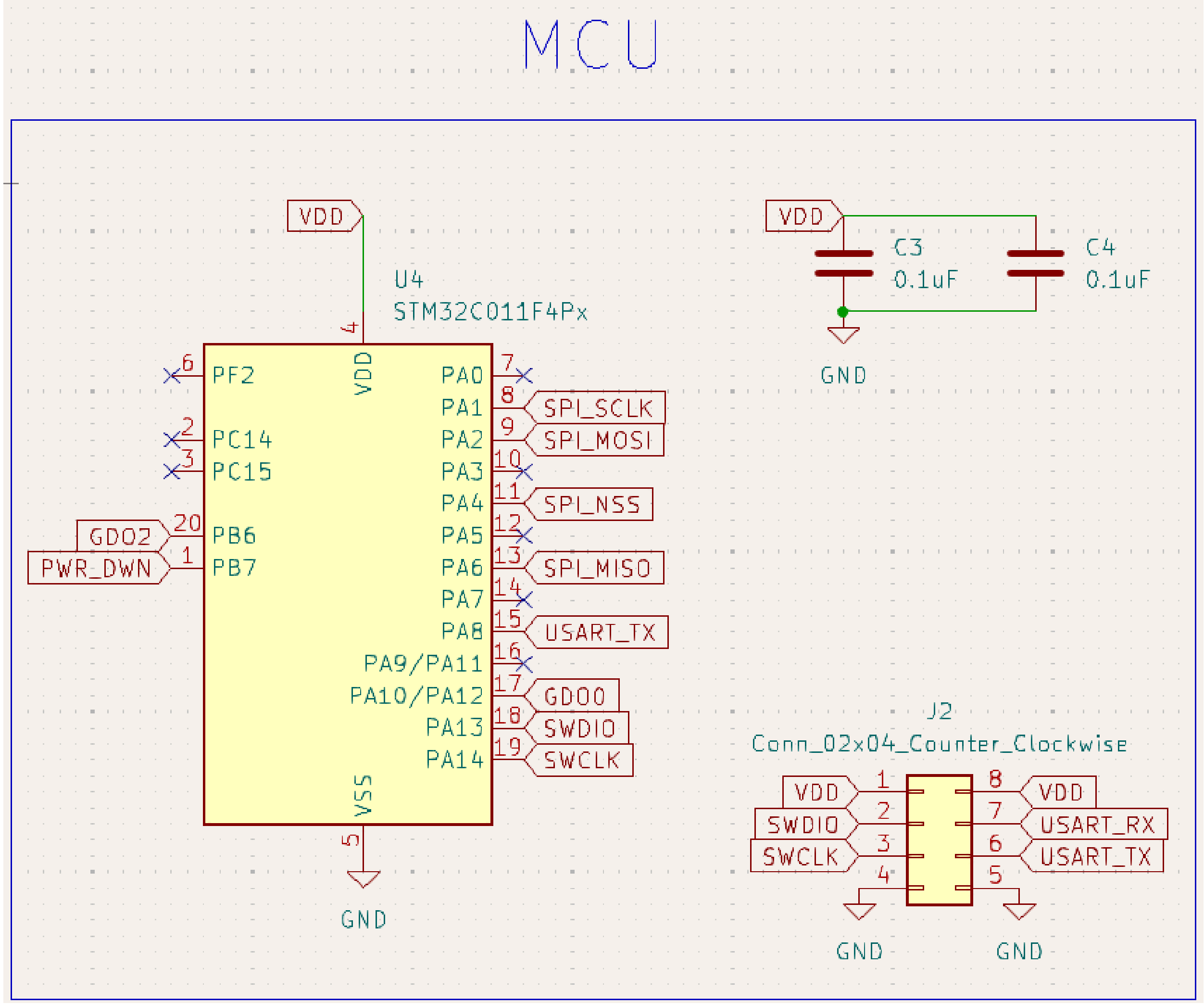


Figure 11 shows circuit schematic for Fob MCU made within KiCad

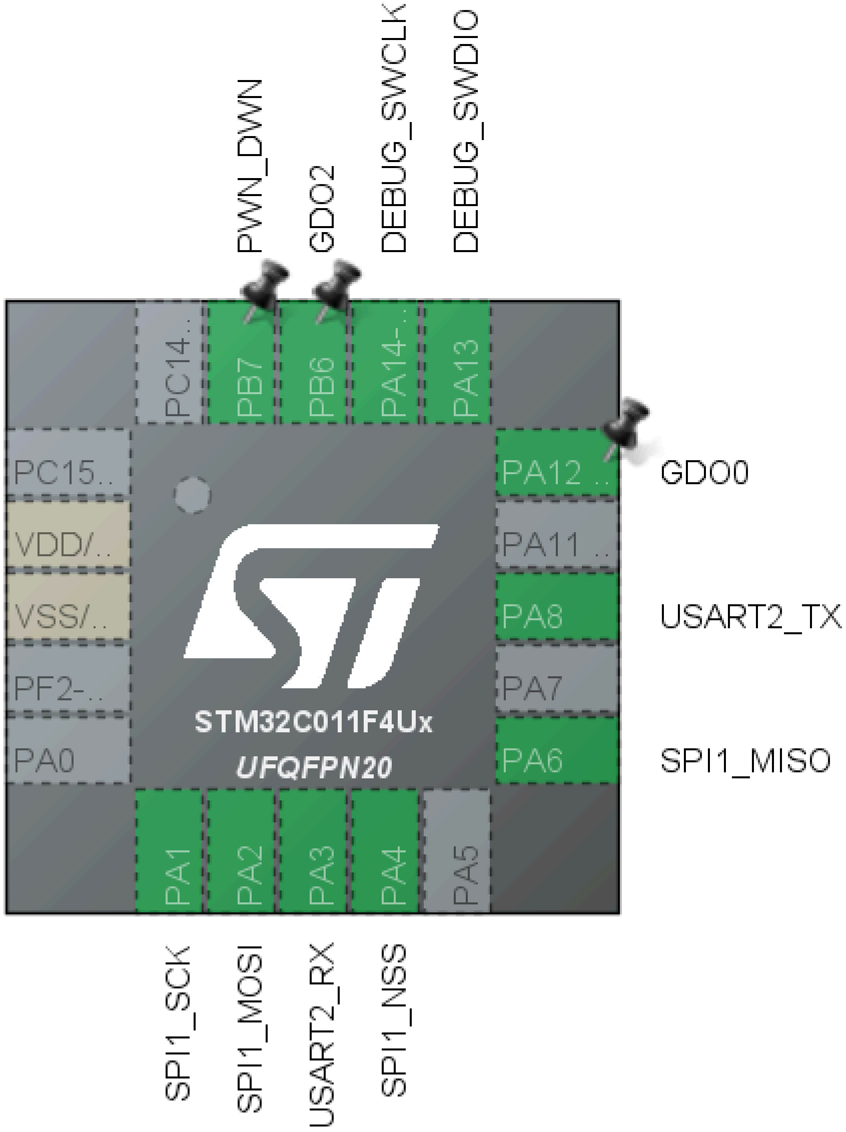


Figure 12 shows the STM32 layout [4]

STM32CubeIDE MCU configuration

STM32CubeIDE Table

Requirements	Verification
MCU can print statements to console via UART-USB converter	Write an MCU program to send a basic “Hello World” message over the UART-USB converter to a laptop.
Schnorr Identification Protocol code implementation can fit on MCU	Verify that the entire software program can fit on the MCU in flash memory (16 KB). If our program is able to compile and run then this will be verified.

Verification and Control Unit (VCU) Overview

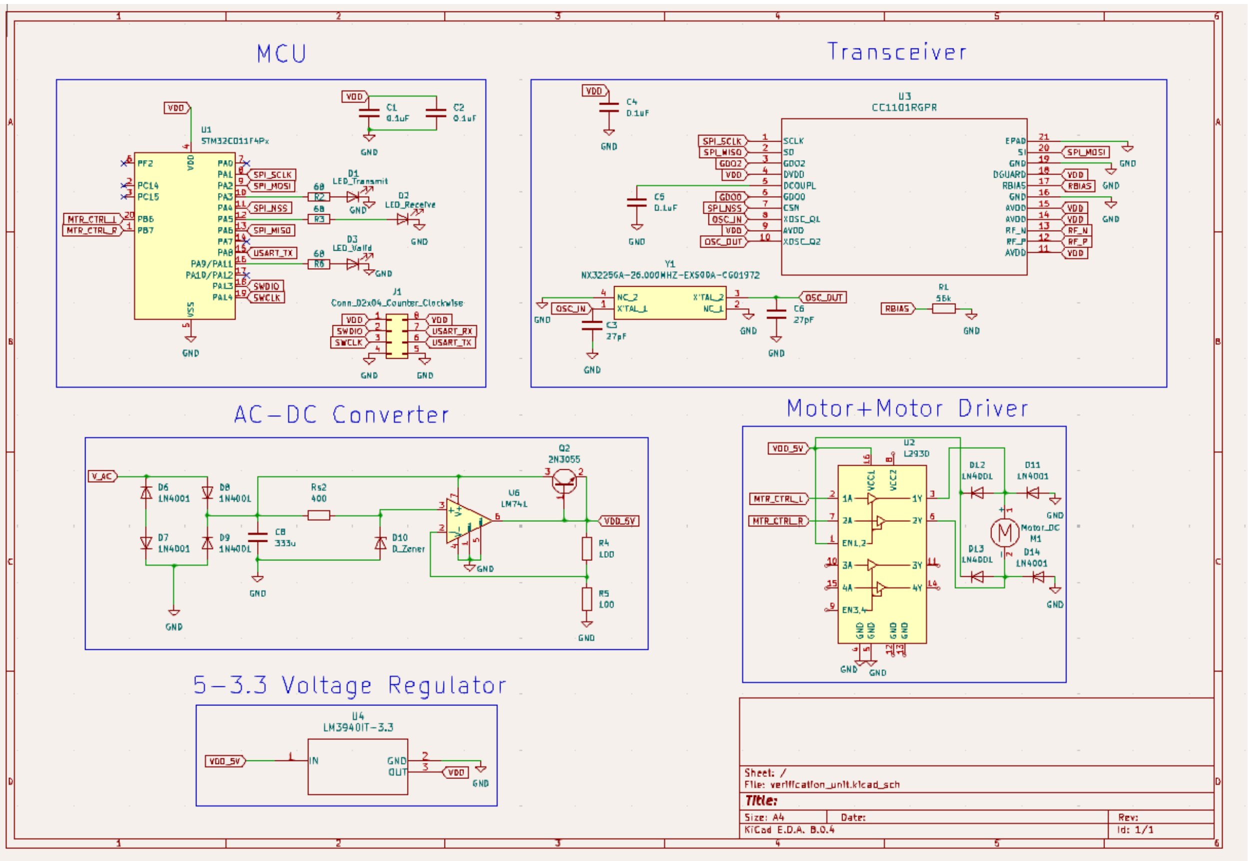


Figure 13 shows the entire Verification and Control Unit (VCU) circuit schematic of our project, consisting of the AC-DC Converter, Motor + Motor Drive, MCU, Transceiver, and a 5 to 3.3 Voltage Regulator, made within KiCad

Verification and Control Unit (VCU) MCU

This MCU is very similar to the MCU on the FOB side where we communicate between the MCU and the transceiver. The main difference between the two is there are a couple of extra output pins being used on the Verification side. PB6 and PB7 both represent the motor control: when PB6 is high and PB7 is low the motor will go left, when vice versa the motor will go right, and when both are high the motor will stop. Additionally I have PA3, PA5, and PA11 connected to LEDs each representing the different states of our VCU: transmitting a signal, receiving a signal, and when a valid unlock sequence has taken place.

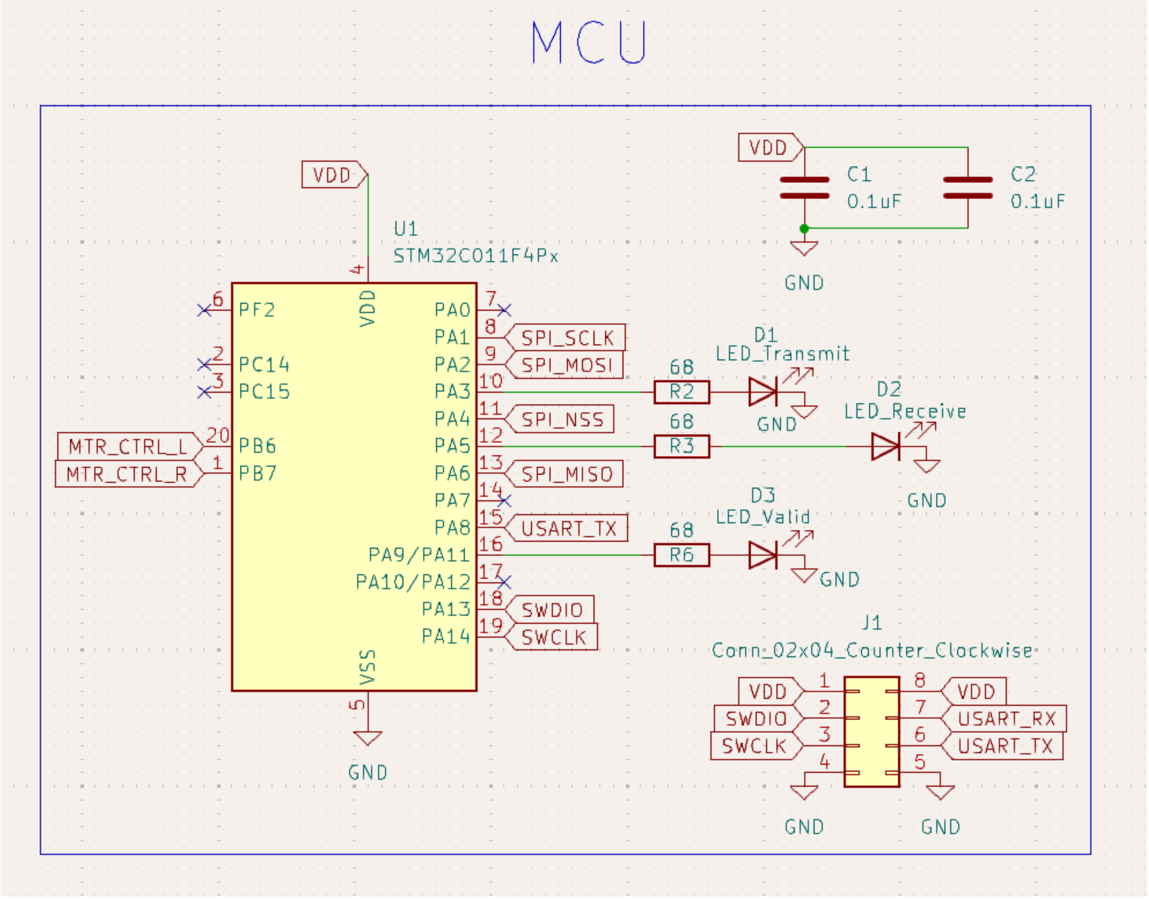


Figure 14 shows the circuit schematic for Verification and Control Unit's MCU made within KiCad

MCU Table

Requirements	Verification
MCU can receive and transmit signals	Write fob software to continuously send a message to the verification and control unit. Verify that the RX LED lights up after a message is sent from the fob. Write verification and control unit code to continuously send messages to the fob. Connect the fob to a PC via the UART-USB converter and verify that for every message we see on the PC, the TX LED is illuminated on the verification and control unit.
MCU can properly control the motor for unlocking	Write code to send basic left and right control signals from the MCU to the L293D motor driver. Essentially we will set MTR_CTRL_L to high, MTR_CTRL_R to high, and the motor should spin left and right respectively. If both are high the motor should not spin.
Schnorr Identification Protocol code implementation can fit on MCU	Verify that the entire software program can fit on the MCU in flash memory (16 KB). If our program is able to compile and run then this will be verified.

Verification and Control Unit (VCU) Power

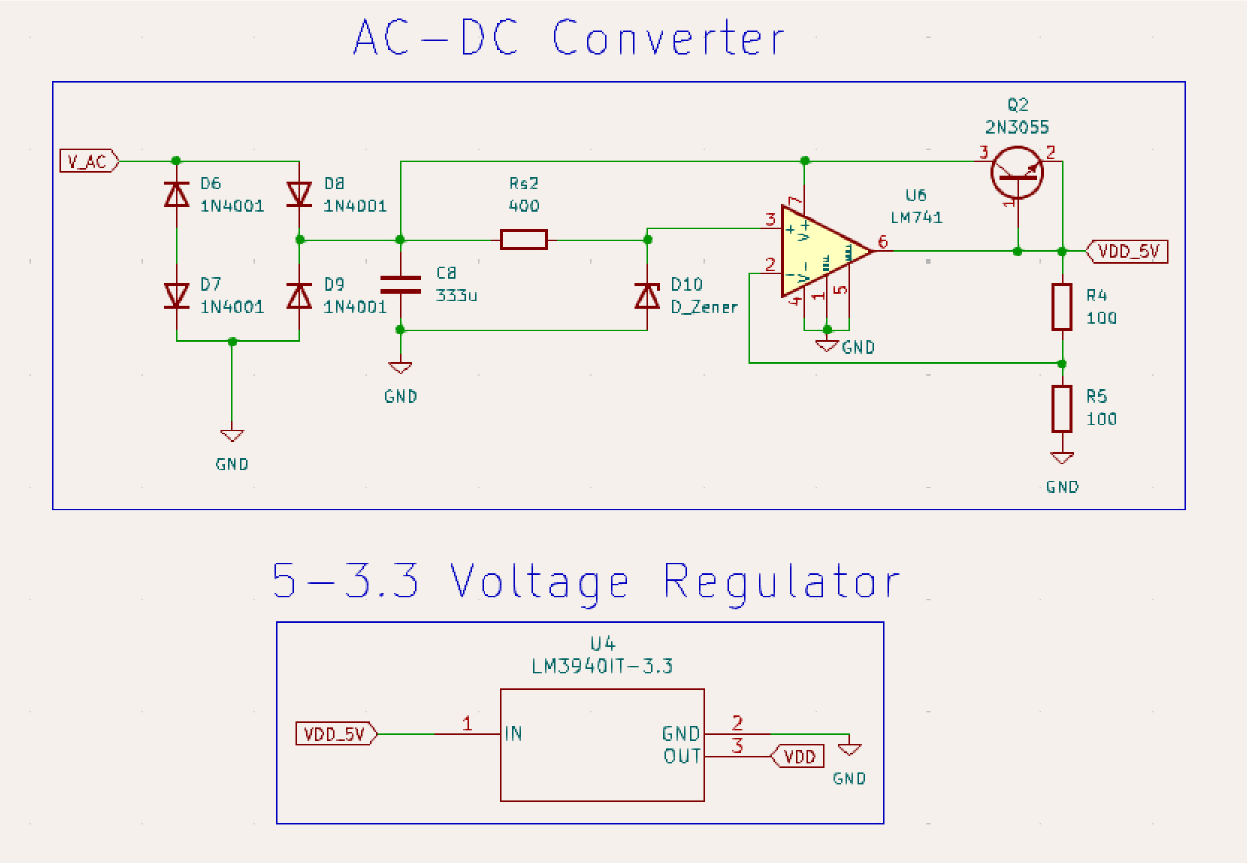


Figure 15 shown above displays the AC-DC power converter as a circuit schematic, utilizing different components for Stepping down voltage, Rectification, Filtering, and Regulation made within KiCad

Our power subsystem for our VCU is very different to our power subsystem on our key FOB. We decided to design our own AC to DC converter, based on the final project of ECE 343 using 1N4001 diodes [6], an op-amp [7] for amplifying the output, along with a 5 to 3.3 LDO regulator [8] to provide the power to our VCU. We know this design works as it worked for our final project from ECE 343.

AC-DC converter and Regulator Table

Requirements	Verification
AD-DC converter converts 120 VAC to around 5VDC AC-DC converter will also output a value of around 1.5 amps to power the motor and other subcomponents.	Will test using an oscilloscope across each stage of conversion: Transformer, Rectifier, Filter, and Regulator. We will test to make sure the signal gets stepped-down, goes through rectification, gets filtered to reduce ripple, and is regulated to achieve a smoothed out DC output, which in this case will be 5 volts. Additionally we still have our ECE 343 circuits

	for comparison and further testing
5 to 3.3 voltage regulator converts voltage properly	We will test this using an oscilloscope to ensure that a 5V in gets converted to a 3.3V out.

Verification and Control Unit (VCU) Motor

Our final subsystem for our VCU is our Motor + Motor Driver. The whole purpose of our motor subsystem is to show a physical output to the unlocking process. We are using a basic 5 volt BLDC motor and a L293D as our motor driver. Our motor driver will take in input from our MCU to control the direction of the motor spin.

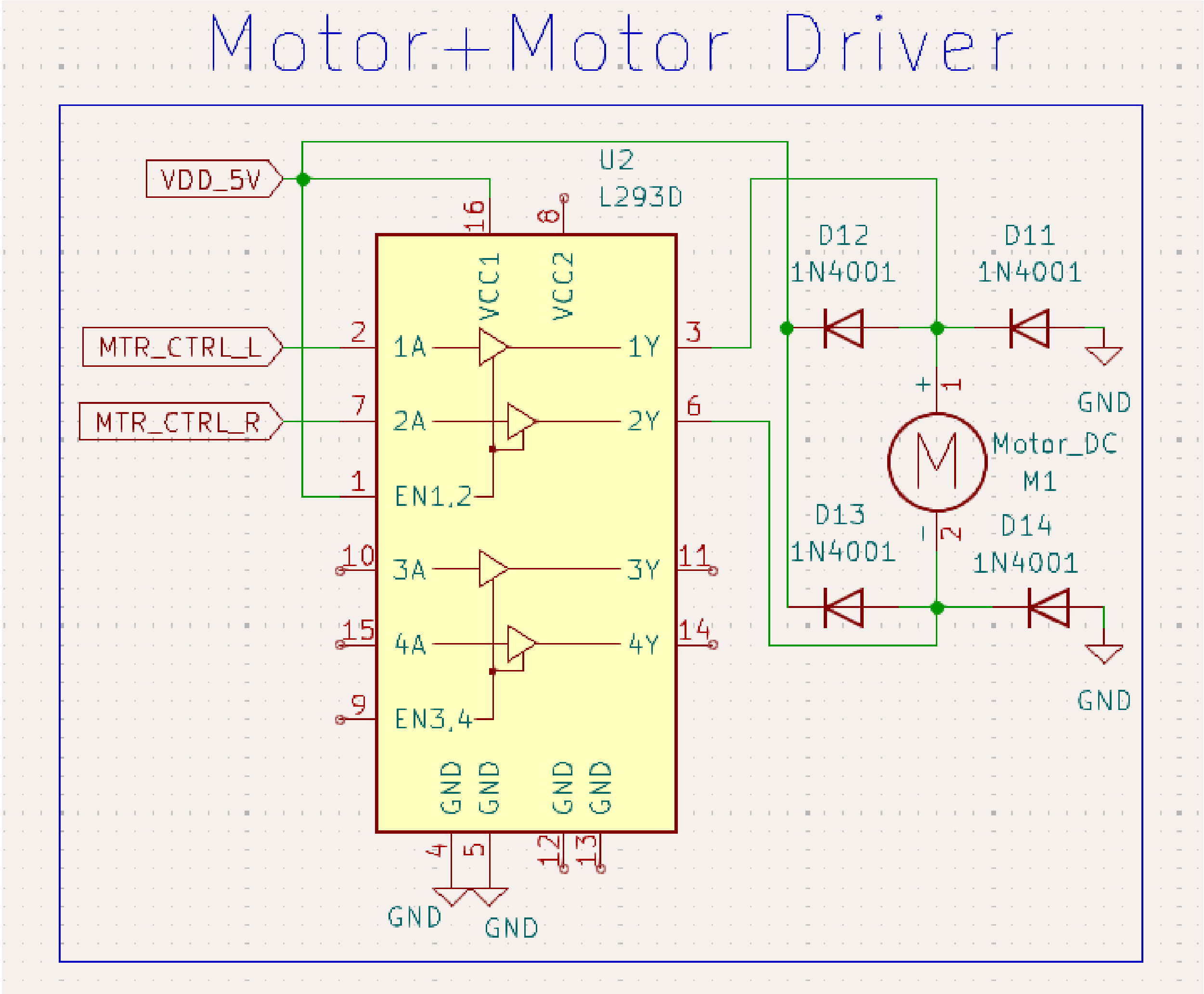


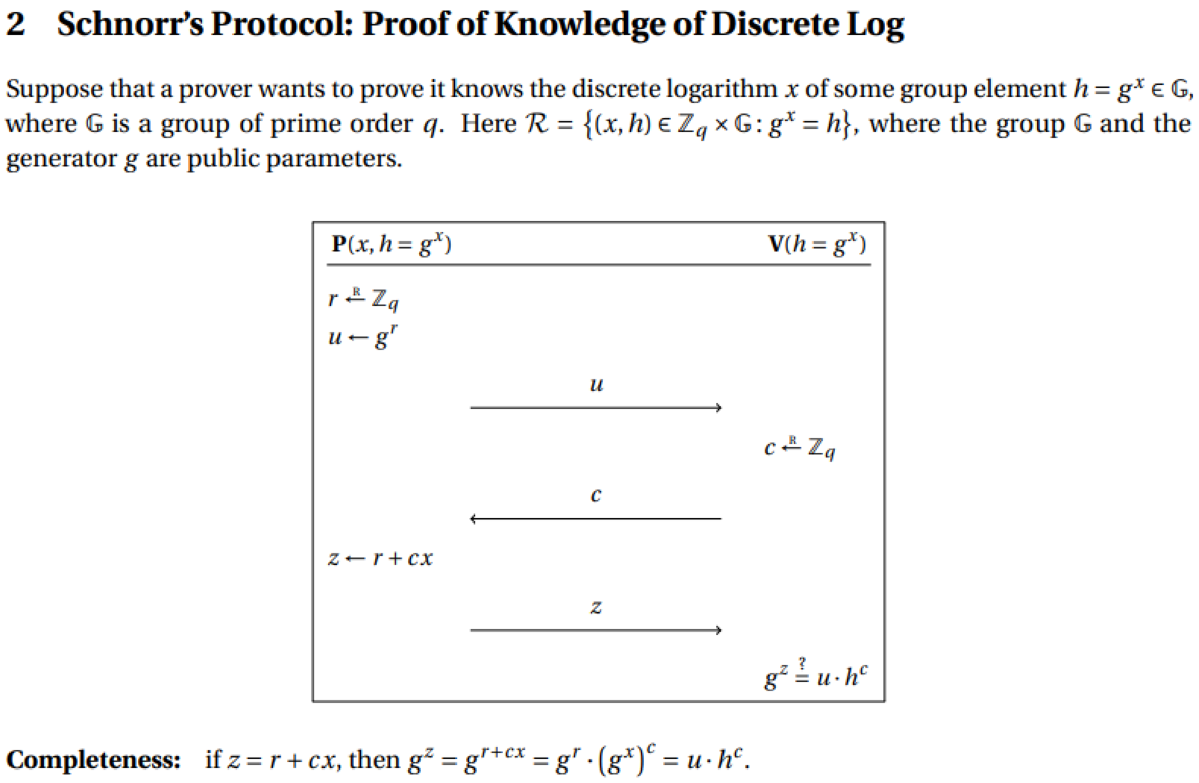
Figure 16 above shows our the circuit schematic of our motor driver and motor [9] made within KiCad

Motor+Motor Driver Table

Requirements	Verification
Motor can spin either in the clockwise or counter clockwise direction during the	Will test sending High to both the 1A and 2A pins of the motor driver to ensure the motor

duration at which it’s receiving a high signal. If pin 1 receives a high, it will turn clockwise, and if pin 2 receives high it will turn counter clockwise.	subsystem works. Note that if both pins receive high or low, the motor will not spin, due to no potential difference across the motor.

Software



2 Schnorr’s Protocol: Proof of Knowledge of Discrete Log

Suppose that a prover wants to prove it knows the discrete logarithm x of some group element $h = g^x \in \mathbb{G}$, where $\mathbb{G}$ is a group of prime order q. Here $\mathcal{R} = \{(x,h) \in \mathbb{Z}_q \times \mathbb{G} : g^x = h\}$, where the group $\mathbb{G}$ and the generator g are public parameters.

$$\begin{array}{lcr} \mathbf{P}(x, h = g^x) & & \mathbf{V}(h = g^x) \\ \hline r \overset{R}{\leftarrow} \mathbb{Z}_q & & \\ u \leftarrow g^r & & \\ & \xrightarrow{\quad u \quad} & \\ & & c \overset{R}{\leftarrow} \mathbb{Z}_q \\ & \xleftarrow{\quad c \quad} & \\ z \leftarrow r + cx & & \\ & \xrightarrow{\quad z \quad} & \\ & & g^z \overset{?}{=} u \cdot h^c \end{array}$$

Completeness: if $z = r + cx$, then $g^z = g^{r+cx} = g^r \cdot (g^x)^c = u \cdot h^c$.

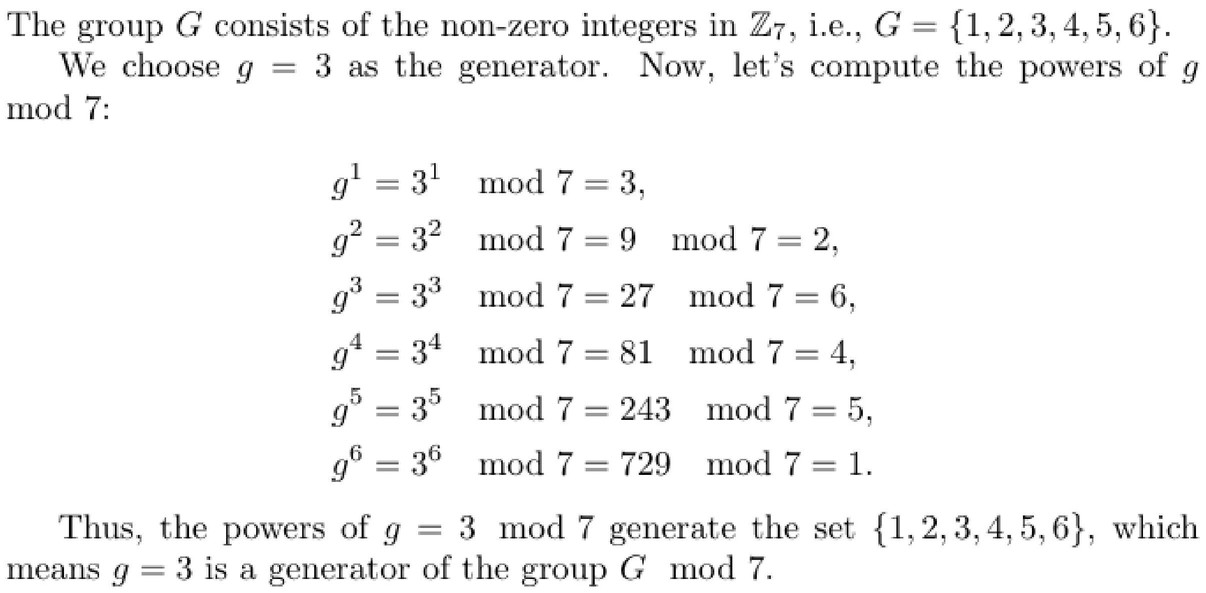
Figure 17 above shows the schnorr protocol sequence [1]

Schnorr Identification Protocol Math

Fob Software

The software which will be run on the fob MCU will take on the role of the prover (P) in the Schnorr identification protocol. This means that the fob will send the initial “open” request, receive a “challenge” wirelessly from the verification and control unit, and then calculate the correct response to the challenge and send it back to the verification and control unit. The fob will be loaded with a public key, $h=g^x$, private key, x, which are both 256 bit numbers, during the initial software flash.

Note that g is the generator of a modular group G. An example would be the group G which has numbers modulo 7. An example is shown below.



The group G consists of the non-zero integers in $\mathbb{Z}_7$, i.e., $G = \{1, 2, 3, 4, 5, 6\}$.

We choose $g = 3$ as the generator. Now, let's compute the powers of g mod 7:

$$\begin{aligned}
g^1 &= 3^1 \mod 7 = 3, \\
g^2 &= 3^2 \mod 7 = 9 \mod 7 = 2, \\
g^3 &= 3^3 \mod 7 = 27 \mod 7 = 6, \\
g^4 &= 3^4 \mod 7 = 81 \mod 7 = 4, \\
g^5 &= 3^5 \mod 7 = 243 \mod 7 = 5, \\
g^6 &= 3^6 \mod 7 = 729 \mod 7 = 1.
\end{aligned}$$

Thus, the powers of $g = 3 \mod 7$ generate the set $\{1, 2, 3, 4, 5, 6\}$, which means $g = 3$ is a generator of the group $G \mod 7$.

Figure 18 above shows further explanation of Schnorr [1]

Modular Group, Generator g Example

When the button is pressed, the fob MCU will generate a random number r within the group G and send $u=g^r$ to the verification and control unit. After receiving the challenge c from the verification and control unit, the fob will compute $z=r + cx$. That computation requires knowledge of the private key x. The fob will then send z to the verification and control unit. If z was correctly computed, then $g^z=u*h^c$. Since g and h are preprogrammed on the verification and control unit, both sides of the equation can be evaluated and if the equation holds, then the unlock command is coming from a fob with an authorized public key.

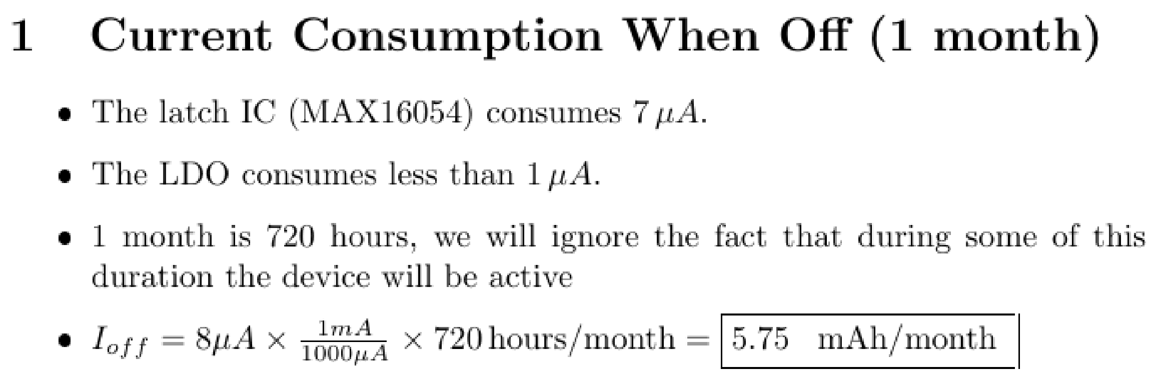
Verification and Control Unit Software

The verification and control unit will be the verifier (V) in the Schnorr Identification Protocol. After receiving the initial “open” command from the fob, we will store it for the final verification calculation. The MCU will generate a random number in group G and send it to the fob as a challenge c. The verification and control unit will then wait for the response z from the fob which it will store and then begin the verification calculation to see if $g^z=u*h^c$. If yes, the verification and control unit will illuminate the “Valid Exchange” LED and then send a signal to the L293D motor driver IC [9] to spin the motor, simulating a garage door opening or car unlocking.

Tolerance Analysis

The subsystem that we have identified which is critical to the success of our project is the battery life of the key fob. In order to achieve our goal of 1 month of battery life, we have to first identify a battery which we will use. Our battery selection requires a battery of 3V, with at least one dimension being smaller than 5 mm. Our battery will need to have a maximum continuous current draw greater than the total amount of active current that our MCU and RF transceiver consume. We must also verify that the quiescent current draw combined with the day to day use of our fob will allow a battery life of at least 1 month.

When in use, the two components in our fob subsystem which will consume the most power are the MCU and the transceiver. We plan on using a power latch IC to provide power to the MCU every time we need to send a message. Since every interaction between the fob and the verification and control system is initiated by a button press, we do not need our system to be in a sleep mode where it can be woken by an interrupt; instead it can be totally off. This means that when our fob is not engaged in an interaction with the verification and control system, we will model our current consumption to be the sum of the currents of the MAX16054 [2] on/off controller latch when off and the LDO [3] when it is not enabled.

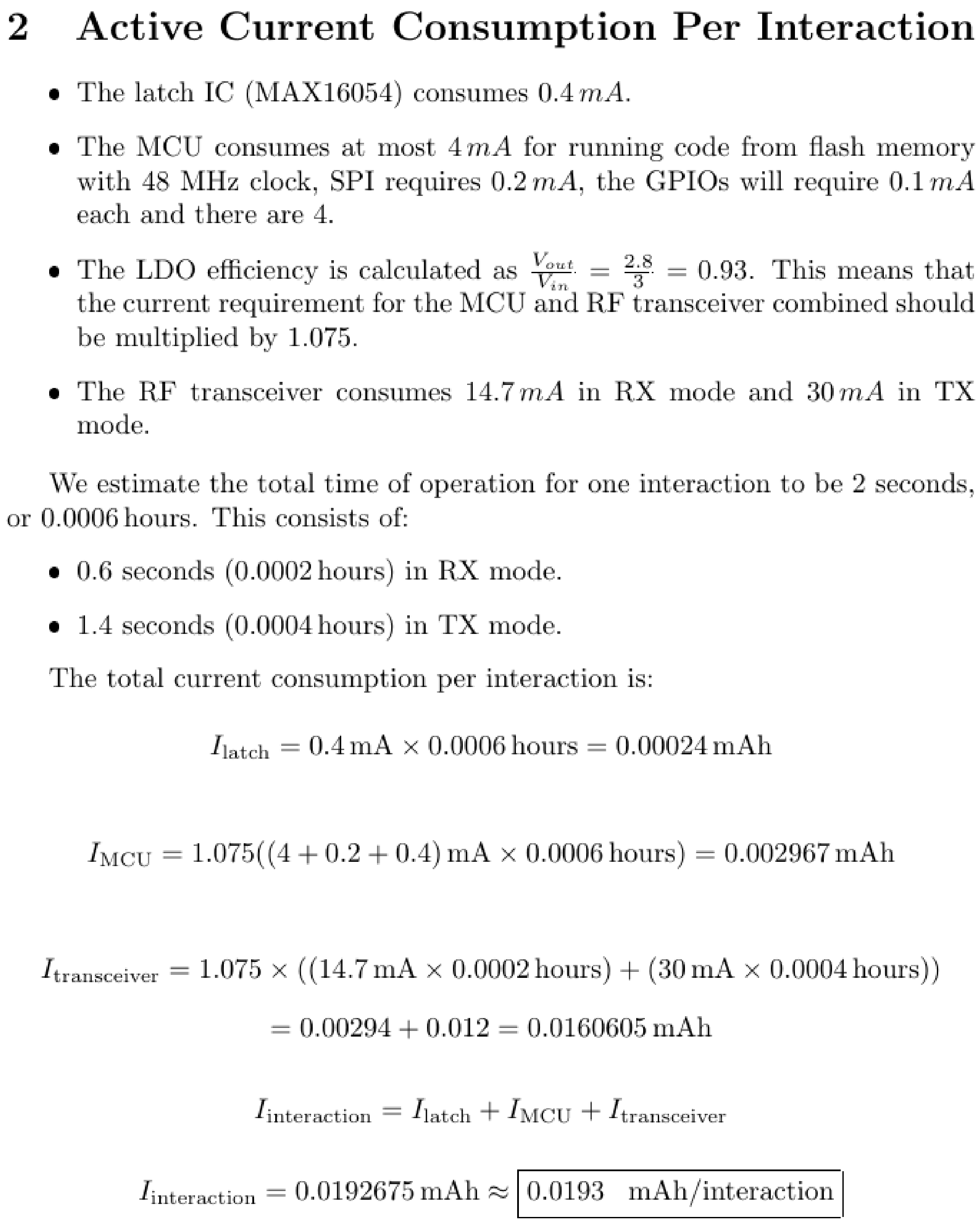


1 Current Consumption When Off (1 month)

- The latch IC (MAX16054) consumes $7\,\mu A$.
- The LDO consumes less than $1\,\mu A$.
- 1 month is 720 hours, we will ignore the fact that during some of this duration the device will be active
- $I_{off} = 8\mu A \times \frac{1mA}{1000\mu A} \times 720\,\text{hours/month} = \boxed{5.75 \quad \text{mAh/month}}$

Figure 19 shows our calculations for how long and how much our device would last

Next, we will calculate the active current consumption (per interaction). This calculation requires some assumptions: the length of each exchange is 2 seconds and for the fob, ⅓ of this time is spent receiving and ⅔ is spent transmitting (the fob has to receive one message and transmit two). The next assumption is that there will be 10 interactions per day between the fob and the verification and control unit.



2 Active Current Consumption Per Interaction

- The latch IC (MAX16054) consumes $0.4\,mA$.
- The MCU consumes at most $4\,mA$ for running code from flash memory with 48 MHz clock, SPI requires $0.2\,mA$, the GPIOs will require $0.1\,mA$ each and there are 4.
- The LDO efficiency is calculated as $\frac{V_{out}}{V_{in}} = \frac{2.8}{3} = 0.93$. This means that the current requirement for the MCU and RF transceiver combined should be multiplied by 1.075.
- The RF transceiver consumes $14.7\,mA$ in RX mode and $30\,mA$ in TX mode.

We estimate the total time of operation for one interaction to be 2 seconds, or 0.0006 hours. This consists of:

- 0.6 seconds (0.0002 hours) in RX mode.
- 1.4 seconds (0.0004 hours) in TX mode.

The total current consumption per interaction is:

$$I_{\text{latch}} = 0.4\,\text{mA} \times 0.0006\,\text{hours} = 0.00024\,\text{mAh}$$

$$I_{\text{MCU}} = 1.075((4 + 0.2 + 0.4)\,\text{mA} \times 0.0006\,\text{hours}) = 0.002967\,\text{mAh}$$

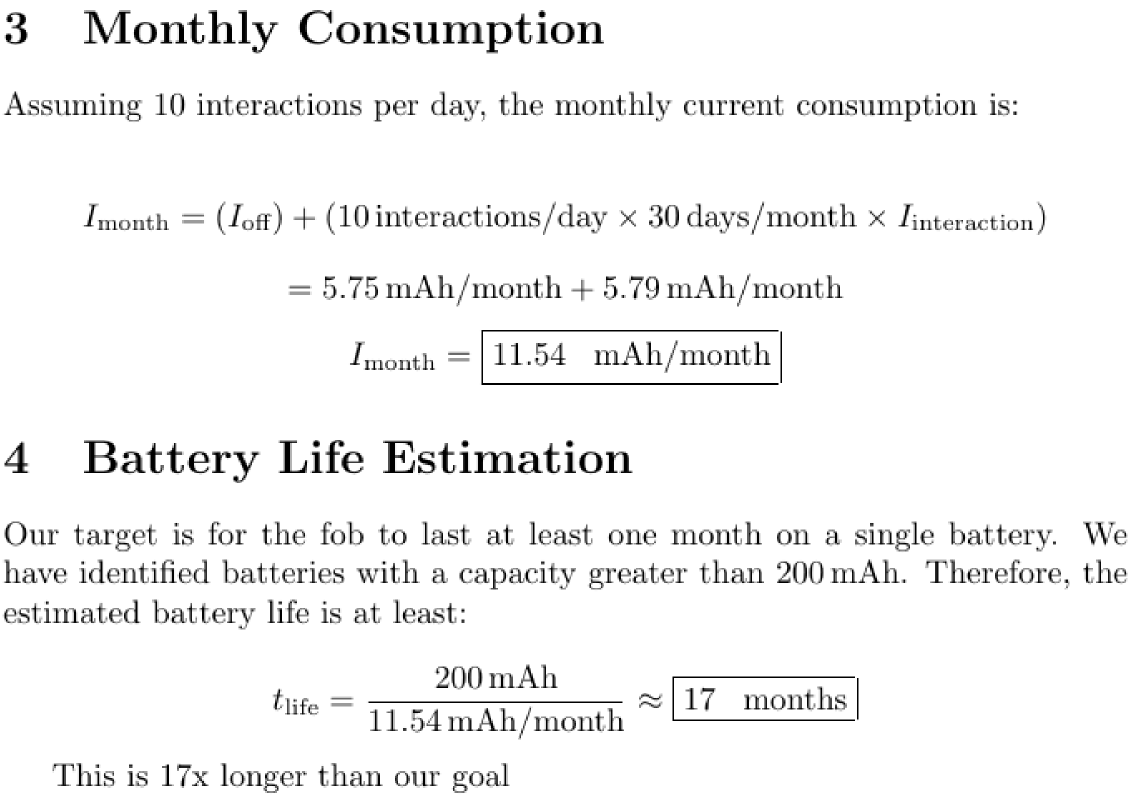
$$\begin{aligned} I_{\text{transceiver}} &= 1.075 \times ((14.7\,\text{mA} \times 0.0002\,\text{hours}) + (30\,\text{mA} \times 0.0004\,\text{hours})) \\ &= 0.00294 + 0.012 = 0.0160605\,\text{mAh} \end{aligned}$$

$$I_{\text{interaction}} = I_{\text{latch}} + I_{\text{MCU}} + I_{\text{transceiver}}$$

$$I_{\text{interaction}} = 0.0192675\,\text{mAh} \approx \boxed{0.0193 \quad \text{mAh/interaction}}$$

Figure 20 shows how much current will be consumed during each interaction/ usage of our fob

Our final calculations are the total current used per month and then how many months our battery will last based on that number.



3 Monthly Consumption

Assuming 10 interactions per day, the monthly current consumption is:

$$
\begin{aligned}
I_{\text{month}} &= (I_{\text{off}}) + (10\,\text{interactions/day} \times 30\,\text{days/month} \times I_{\text{interaction}}) \\
&= 5.75\,\text{mAh/month} + 5.79\,\text{mAh/month} \\
I_{\text{month}} &= \boxed{11.54 \quad \text{mAh/month}}
\end{aligned}
$$

4 Battery Life Estimation

Our target is for the fob to last at least one month on a single battery. We have identified batteries with a capacity greater than 200 mAh. Therefore, the estimated battery life is at least:

$$t_{\text{life}} = \frac{200\,\text{mAh}}{11.54\,\text{mAh/month}} \approx \boxed{17 \quad \text{months}}$$

This is 17x longer than our goal

Figure 21 shows our calculations for finding the duration of the battery we are using and overall and lifetime of the device before needing a new battery.

Cost and Schedule

Schedule

Week	Task	Person
October 6- October 12	Finish up designing schematics for components for the Fob, and have PCB designed (Power, MCU, 315 MHz Transceiver)	Michael
	Finish up designing schematics for Verification and Control (VCU) (315 MHz Transceiver, MCU, H-Bridge IC)	Vasav
	Finish up designing schematics for Verification and Control (VCU) (LDO, and AC-DC Converter)	Pedro
	Review each others' designs	Everyone
October 13 - October 19	Begin ordering parts for both systems	Everyone
	Make sure Fob PCB Design is ready	Michael
	Make sure VCU PCB Design is ready	Vasav
	Make sure VCU PCB Design is ready	Pedro
	PCBWAY FIRST ROUND AUDIT BEFORE 10/15 AT 4:45 PM	Everyone
October 20 - October 26	While waiting for PCBs to come, testing systems on breadboards.	Everyone
	Create and test Fob system using breadboards to test functionality (Power, MCU, 315 MHz Transceiver)	Michael
	Create and test VCU system using breadboards to test functionality (315 MHz Transceiver, MCU, H-Bridge IC)	Vasav
	Create and test VCU system using breadboards to test functionality (315 MHz Transceiver, LDO, and AC-DC Converter)	Pedro
	PCBWAY SECOND ROUND AUDIT BEFORE 10/15 AT 4:45 PM	Everyone
October 27 - November 2	Soldering Fob system components onto Fob PCB and begin testing individual systems	Michael
	Soldering Verification and Control system components onto VCU PCB and begin testing individual systems.	Vasav
	Soldering Verification and Control system components onto VCU PCB and begin testing individual systems	Pedro
	PCBWAY THIRD ROUND AUDIT BEFORE 11/4 AT 4:45 PM	Everyone
November 3 -	Testing and troubleshooting that both systems work together. Fix and implement new designs for correcting functionality.	Everyone

November 9	Test, troubleshoot, record findings, and fix issues within Fob system	Michael
	Test, troubleshoot, record findings, and fix issues within the VCU system	Vasav
	Test, troubleshoot, record findings, and fix issues within the VCU system	Pedro
	PCBWAY FOURTH ROUND AUDIT BEFORE 11/4 AT 4:45 PM	Everyone
November 10 - November 16	Testing and troubleshooting that both systems work together. Fix and implement new designs for correcting functionality.	Everyone
	Test, troubleshoot, record findings, and fix issues within Fob system.	Michael
	Test, troubleshoot, record findings, and fix issues within the VCU system.	Vasav
	Test, troubleshoot, record findings, and fix issues within the VCU system.	Pedro
November 17 - November 23	Finish up Fob Unit	Michael
	Finish up VCU	Vasav
	Finish up VCU	Pedro
	MOCK DEMO THIS WEEK DURING TA MEETING. MAKE SURE BOTH FOB AND VCU ARE COMMUNICATING WITH EACH OTHER	Everyone
November 24 - November 30	Fall break, Make any final changes/ updates to Fob Unit, begin working on Final Presentation and Final Report.	Michael
	Fall break, Make any final changes/ updates to VCU, begin working on Final Presentation and Final Report.	Vasav
	Fall break, Make any final changes/ updates to VCU, begin working on Final Presentation and Final Report.	Pedro
December 1 - December 7	**FINAL DEMO WITH TA AND INSTRUCTORS**	Michael
	FINAL DEMO WITH TA AND INSTRUCTORS	Vasav
	FINAL DEMO WITH TA AND INSTRUCTORS	Pedro
December 9 - December 10	PRESENT FINAL PRESENTATION AND FINISH REPORT	Michael
	PRESENT FINAL PRESENTATION AND FINISH REPORT	Vasav
	PRESENT FINAL PRESENTATION AND FINISH REPORT	Pedro
December 11	**FINAL REPORT DUE AT 11:59PM**	Everyone

Cost Analysis

Team member compensation

$\$40\ *\ 2.5\ *\ 50\ =\ \$5000\ each$

$\$5000\ *\ 3\ members\ =\ \$15000$

Fob Unit		
Description	**Manufacturer**	**Cost**
RF ANT 315MHZ HELICAL SOLDER SMD	TE Connectivity Linx	$1.18
SWITCH PUSH SPST-NO 0.1A 32V	C&K	$1.29
IC RF TXRX ISM<1GHZ 20QFN	Analog Devices Inc./Maxim Integrated	$4.30
IC RF TXRX ISM<1GHZ 20QFN	Texas Instruments	$3.63
BATTERY HOLDER COIN 20MM SMD	MPD (Memory Protection Devices)	$1.24
IC MCU 32BIT 16KB FLASH 20TSSOP	STMicroelectronics	$1.71
IC REG LINEAR 2.8V 200MA SC70-5	Texas Instruments	$0.15
CRYSTAL 26.0000MHZ 10PF SMD	NDK America, Inc.	$0.66
Total		**$14.16**

VCU		
Description	**Manufacturer**	**Cost**
R280 3-6V 12000RPM BRSHD DC MTR	OSEPP Electronics LTD	$4.45
IC MCU 32BIT 16KB FLASH 20TSSOP	STMicroelectronics	$1.71
16 Pin Motor Driver IC, 4.5-36V @1A, L293D	Texas Instruments	$2.95
IC RF TXRX ISM<1GHZ 20QFN	Texas Instruments	$3.63
IC REG LINEAR 3.3V 800MA TO220-3	Texas Instruments	$1.79

VCU		
CRYSTAL 26.0000MHZ 10PF SMD	NDK America, Inc.	$0.66
Total		**$15.19**

$Total\ Parts\ Cost\ =\ \$15.19\ +\ \$14.16\ =\ \$29.35$

Assume a 5% shipping cost: $Shipping\ =\ \$29.35\ *\ 5\%\ =\ \$1.47$

Assume 10% sales tax: $Tax\ =\ \$29.35\ *\ 10\%\ =\ \$2.94$

$Final\ Total\ Cost\ =\ Team\ Member\ Compensation\ +\ Total\ Parts\ Cost\ +\ Shipping\ +\ Tax$

$Final\ Total\ Cost\ =\ \$15,000\ +\ \$29.35\ +\ \$1.47\ +\ \$2.94\ =\ \$15,033.76$

Ethics and Safety

Potential Ethical breaches:

One ethical concern we have is the RF interference of the transceiver, we will ensure that our transceiver adheres to the FCC requirements: 787 kHz bandwidth and 200 uV/m at 3 m distance.

Potential safety concerns:

Energy Converter: Since we are using an AC-DC converter, we need to make sure our converter properly converts the 120V AC, typical for wall outlets, to our desired voltage required for our garage door lock to function properly. The only possible safety concern is if we incorrectly build our converter, but with proper failsafes (designing fuses and grounds into our pcb) and schematics that concern will be addressed. We also need to make sure that our model garage door locks and unlocks in a reasonable amount of time, not taking too long so that if the user needs to access, it unlocks quickly.

Fob BOM

Reference	Value	Footprint	Qty	Link(non-standard)	Price (non-standard)
C1,C2	1uF	Capacitor_SMD:C_0603_1608Metric	2		
C3,C4,C5,C8,C9	0.1uF	Capacitor_SMD:C_0603_1608Metric	5		
C6,C7	27pF	Capacitor_SMD:C_0402_1005Metric	2		
C10,C13	220pF	Capacitor_SMD:C_0402_1005Metric	2		
C11,C12,C14	6.8pF	Capacitor_SMD:C_0402_1005Metric	3		
C15	12pF	Capacitor_SMD:C_0402_1005Metric	1		
E1	ANT-315-HESM	ANT-315-HESM:XDCR_ANT-315-HESM	1	Link	$1.18
J2	Conn_02x04_Counter_Clockwise	Connector_PinSocket_2.54mm:PinSocket_2x04_P2.54mm_Vertical	1		
L1,L3,L4	33nH	Inductor_SMD:L_0402_1005Metric	3		

L2	18nH	Inductor_SMD:L_0402_1005Metric	1		
R1	56k	Resistor_SMD:R_0402_1005Metric	1		
R2	10k	Resistor_SMD:R_0402_1005Metric	1		
S1	D6C90F2LFS	SamacSys_Parts:D6C90F2LFS	1	Link	$1.29
U1	MAX16054AZT_T	MAX16054AZT_T:SOT95P275X110-6N	1	Link	$4.30
U2	CC1101RGPR	CC1101:RGP20_2P4X2P4	1	Link	$3.63
U3	BU2032SM-JJ-GTR	SamacSys_Parts:BU2032SMJJGTR	1	Link	$1.24
U4	STM32C011F4Px	Package_SO:TSSOP-20_4.4x6.5mm_P0.65mm	1	Link	$1.71
U5	TLV70028_SOT353	Package_TO_SOT_SMD:SOT-353_SC-70-5	1	Link	$0.15
Y1	NX3225GA-26.000MHZ-EXS00A-CG01972	SamacSys_Parts:NX3225GA16000MSTDCRG1	1	Link	$0.66

Verification and Control Unit BOM

Reference	Value	Footprint	Qty	Link(non-standard)	Price (non-standard)
C1,C2,C4,C5	0.1uF	Capacitor_SMD:C_0603_1608Metric	4		
C3,C6	27pF	Capacitor_SMD:C_0402_1005Metric	2		
C8	333u		1		
D1	LED_Transmit		1		
D2	LED_Receive		1		
D3	LED_Valid		1		
D6,D7,D8,D9,D11,D12,D13,D14	1N4001	Diode_THT:D_DO-41_SOD81_P10.16mm_Horizontal	8		
D10	D_Zener		1		
J1	Conn_02x04_Counter_Clockwise	Connector_PinSocket_2.54mm:PinSocket_2x04_P2.54mm_Vertical	1		
M1	Motor_DC		1	Link	$4.45
Q2	2N3055	Package_TO_SOT_THT:TO-3	1		
R1	56k	Resistor_SMD:R_0402_1005Metric	1		
R2,R3,R6	68		3		
R4,R5	100		2		
Rs2	400		1		

U1	STM32C011F4Px	Package_SO:TSSOP-20_4.4x6.5mm_P0.65mm	1	Link	$1.71
U2	L293D	Package_DIP:DIP-16_W7.62mm	1	Link	$2.95
U3	CC1101RGPR	CC1101:RGP20_2P4X2P4	1	Link	$3.63
U4	LM3940IT-3.3	T03B	1	Link	$1.79
U6	LM741	http://www.ti.com/lit/ds/symlink/lm741.pdf	1		
Y1	NX3225GA-26.000MHZ-EXS00A-CG01972	SamacSys_Parts:NX3225GA16000MSTDCRG1	1	Link	$0.66

Citations

[1] Dima Kogan (2019), “Lecture 5: Proofs of Knowledge, Schnorr’s protocol, NIZK”, CS355, Computer Science Department, Stanford University [Online]. Available: https://crypto.stanford.edu/cs355/19sp/lec5.pdf

[Accessed: Sept. 30, 2024]

[2] Maxim Integrated Products, “On/Off Controller with Debounce and ±15kV ESD Protection”, Rev 0, May 2008 [Online]. Available: https://www.analog.com/media/en/technical-documentation/data-sheets/MAX16054.pdf

[3] Texas Instruments, “200-mA, Low-IQ, Low-Dropout Regulator (LDO) for Portable Devices”, Rev C, June 2018 [Online]. Available: https://www.ti.com/lit/ds/symlink/tlv700xx-q1.pdf?ts=1727978597283&ref_url=https%253A%252F%252Fwww.google.com%252F

[4] STMicroelectronics, “STM32C011x4/x6”, Rev. 4, Jan. 2024 [Online]. Available: https://www.st.com/en/microcontrollers-microprocessors/stm32c011f4.html

[5] Texas Instruments, “Low-Power Sub-1 GHz RF Transceiver”, Revision SWRS061I, Nov. 2013 [Online]. Available: https://www.ti.com/lit/ds/symlink/cc1101.pdf?ts=1727939599209&ref_url=https%253A%252F%252Fwww.ti.com%252Fproduct%252FCC1101

[6] Onsemi, “Axial-Lead Glass Passivated Standard Recovery Rectifiers”, Rev.18, June 2024 [Online]. Available: https://www.onsemi.com/pdf/datasheet/1n4001-d.pdf

[7] Texas Instruments, “LM741 Operational Amplifier”, Rev D, Oct. 2015 [Online]. Available: https://www.ti.com/lit/ds/symlink/lm741.pdf

[8] Texas Instruments, “LM3940 1-A Low-Dropout Regulator for 5-V to 3.3-V Conversion”, Rev. G, Feb. 2015 [Online]. Available: https://www.ti.com/general/docs/suppproductinfo.tsp?distId=10&gotoUrl=https%3A%2F%2Fwww.ti.com%2Flit%2Fgpn%2Flm3940

[9] Texas Instruments, “L293x Quadruple Half-H Drivers “, Rev.D, Jan. 2016 [Online]. Available: https://www.ti.com/lit/ds/symlink/l293d.pdf?ts=1727938192243&ref_url=https%253A%252F%252Fwww.ti.com%252Fproduct%252FL293D