Key Master

RFID Based Key Choosing System

"These keys are lit."

Team 14

Team Members:
Petar Barac
Amanda Beck
Leslie Cheng

TA:
Jacob Bryan

March 9, 2017

1 Introduction

1.1 Objective

There are many doors that need to be opened, but trying to match keys to the correct doors and locks can be difficult. For the everyday use, an individual will learn which key is for what purpose through a combination of repetition and memorization, but there is still a limit to how many key/lock combinations one person can commit to memory. For individuals that carry a dozen plus keys, the task of finding the right key can be frustrating and time consuming. Professions that tend to carry key rings include landlords, maintenance workers, and groundskeepers, which may work on a number of properties that do not have upgraded features like electronic locks or even the ability to create master keys to serve many purposes. Individuals in this situation could benefit from a cost effective and time-saving product that identifies the correct key for them.

The Key Master will eliminate the need for guessing by identifying the corresponding key for a door. Instead of upgrading door locks, this system will work with any basic key and lock combination. RFID tags, each with distinct frequencies, can be discretely added near a lock, and each will match with one of the key holders on a key ring. The Key Master key ring will the let the user know the correct key by illuminating an embedded LED on the key holder.

1.2 Background

With large numbers of keys, efficiently identifying which key belongs to a lock can be difficult and defaults to trial and error. The more keys involved, the longer this process will take especially if multiple locks need to be accessed in short succession. Another problem that could delay entry is if the area has little lighting. Tags or markings matching doors with keys or the keys themselves might not be fully visible, so some error is possible in identifying the correct key by distinct features. Another option is replacing all the locks with matching ones that could use a master key to open. This involves a lot of additional cost that may not be feasible, as that upgrade will cost at least $15 per door and can add up for larger buildings.

Electronic locks is another option for making access easier because one keycard can be programmed to open all the locks, but this again would incur upgrade costs. Additionally, older buildings with physical locks would require additional installations to provide power for the new locks, not to mention the expense of electronic locks (over $1000 per lock for those in the ECEB [1]). These locks are most useful for high traffic locations with multiple restricted areas because keycards with individual access to areas is logistically simpler and safer than having keys given to and retrieved from many individuals.

1.3 High-level requirements list

- Reliably identifies the correct key for its corresponding RFID tag.
- Battery life lasts for a day with multiple readings taken per hour.
- New keys can be added to the system as needed.

2 Design

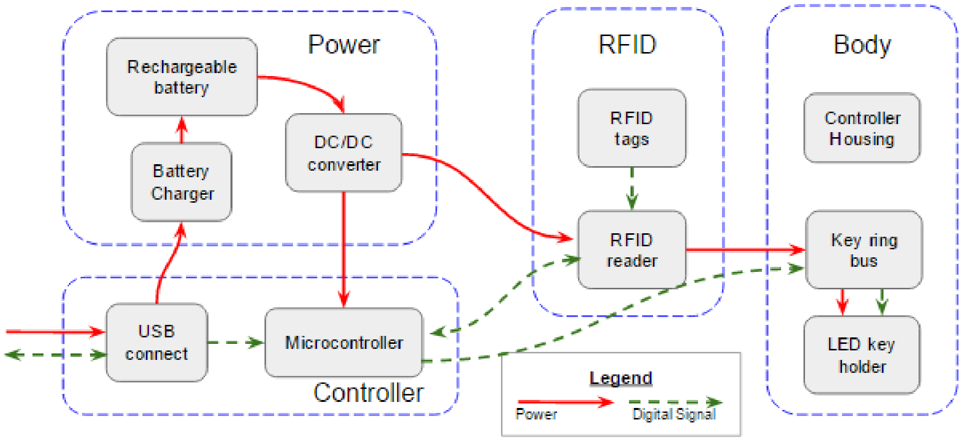

Figure 1: Block diagram of Key Master components.

The Key Master consists of four main modules that will allow for proper operation: Controller, Transmitter/Receiver, Power, and Body. The most important module is the Transmitter/Receiver will read the RFID tags near the locks and will transmit a pulse to the keys given the correct frequency. The controller module stores the frequency information about a key/lock pair and relays the information to the other modules. The power module will provide consistent low power to all the modules but be able to handle the short bursts of power needs when the transmitter and receiver. Finally, the body module encompasses the design which connects the keys to the controls via a key ring bus.

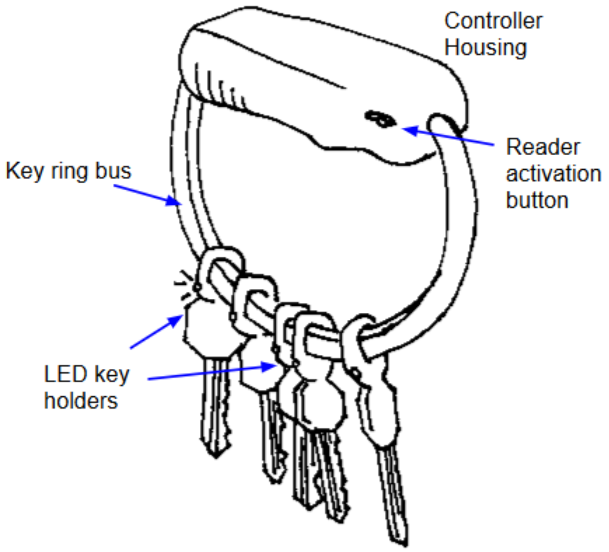

Figure 2: Sketch of the intended physical design of the system.

Fig. 2 illustrates the design of the Key Master. At the top is the controller housing, which will actually hold the power, controller, and transmitter/receiver and doubles as a hand grip. A button for activating the RFID reader will help allow the unit to last all day but meet the immediate demands of the user. The keyring will be attached to and loop around that housing. Ideally, the keyring will have an easy disconnect so keys can easily be added and removed if needed. Key holders fit snuggly on the key ring bus, and the bus will be protected by an outer insulated layer to protect the user. Each key holders will fit around the head of a key and house an LED for signaling the user.

2.1 Controller

The controller module is responsible for interfacing the RFID reader and 1-Wire chips in the keys. It will read the value in the RFID tag and match it to the key, and it can also write to the RFID tag in order to add and match new keys to the system.

2.1.1 Microcontroller Unit

The microcontroller unit (MCU) will serve essentially as a lookup table for the RFID reader. The reader will send the data from the tag to the microcontroller where it will access memory to find the associated key. Each DS2413 chip associated with each key has an unique 64-bit address to access.

$$100 \text{ keys} \rightarrow 100\text{chips} \times 64\frac{\text{bits}}{\text{chip}} = 6,400 \text{ bits} = 800 \text{ bytes} \tag{1}$$

The MCU also can use the RFID reader to change the value of the RFID tag while adding a key. After inserting a key into the new key port and pressing the button, the MCU will read the address of the 1-Wire chip of the new key and store that value into the RFID tag.

Requirement	**Verification**
Be able to receive and output at least 64 bits through one pin.	1. Insert simple program into microcontroller that will receive a 64 bit input and print 64 bits. 2. Have program read input at an I/O pin as an individual bit on the leading edge of a signal at a separate pin to be used as the "clock". 3. Manually input 64 bit value using a 5V DC signal as the bits while using the other pin to signal when to read the input. 4. Have the microcontroller print the 64 bit input by lighting an LED for every 1 bit by cycling from the most to least significant bit by using the "clock" pin.
Must be able to run at least 1 MIPS (million of instructions per second)	1. Create a simple program with a loop that ends after 10 million instructions. 2. Start timer at the same time the loop starts. 3. Record time needed to execute all instructions. 4. Divide time by 10 for an average time needed for 1 million instructions. 5. Repeat five times to verify speed meets or exceeds requirements.

2.1.2 USB Interface

The USB interface is the main way of accessing the controller as well as charging the system. This allows a universal charging solution in line with most phone chargers or through a computer. The intended low power consumption of the system means the USB interface is adequate for our purposes since a standard USB port outputs up to 0.5 A at 5 V for USB 2.0 [2].

2.2 Radio Frequency Identification

This module is responsible for identifying RFID tags at 125kHz. After identifying the tag, it processes the data from the tag in the microcontroller unit.

2.2.1 RFID Tags

The RFID tags should ideally be as small as possible while still being adhesive enough to stick onto a door or near a lock. The tags will be used to identify which door, and each one should be uniquely identifiable so that different doors can identified.

Requirement	Verification
The tag must be able to be read when the reader tag is placed directly above it and at most be able to read the tag from 3 inches away.	1. Connecting the reader to the Arduino and displaying the output of the reader on a computer screen. 2. Bring the reader 3 inches above the tag. Check the output of the reader, if the output reads the default output of xFEEDFACE then the tag is being read. 3. If the tag has already been written with an output, then if that output is read this tag has been properly identified

2.2.2 RFID Reader

The RFID reader is an antenna that is responsible for identifying the RFID tag and assess which key is necessary to open it. This component will most likely consume the bulk of the power but nonetheless is the most integral part in identifying the proper key for the identified lock.

Requirement	Verification
The reader must be able to read data from a tag within 2 seconds of being turned on.	1. Connect reader through Arduino to computer while RFID reader is unpowered. 2. Have RFID tag next to reader. 3. Simultaneously connect power to reader and run program while timing how long until RFID contents are read. 4. Repeat five times to verify read time of 2 or less seconds.

2.3 Power

Power is required to keep the individual modules ready to operate multiple times a day. Each element will require about 5V, and will require a higher current draw when reading RFID tags.

2.3.1 Rechargeable Battery

To last all day with multiple key identifications, a rechargeable battery will need to provide sufficient power to the unit. All of the components require a 5V input. Given multiple units that will draw up to 600 mA of current during each operation, the battery will need to provide sufficient mAh to last after 100 operations over an eight hour period. It is also important that the power source be compact enough to fit in a handgrip-sized housing attached to the key ring.

Expected timeframe of max operations over 8 hours:	30 seconds × 100 reads × $\frac{\text{1minute}}{\text{60seconds}}$ = 50 minutes
Expected current draw by elements:	200mA (RFID reader) + 3.6mA (controller) + 20mA (LED)= 223.6mA for active
Remainder time:	$7\frac{1}{6}$ hours
Inactive current draw:	10mA (RFID) + 1mA (contrller) = 11 mA
	223.6mA $\times\frac{5}{6}$ hour + 11 mA (nominal) × $7\frac{1}{6}$ hour = 265.17 mAh

Requirement	Verification
Must provide a minimum of 300mAh over an eight hour period with a minimum of 5.5 V as final discharge voltage and no more than 300mA drawn during the operations	1. Measure starting, full charge battery voltage as reference. 2. Run operations with 25, 50, and 100 read cycles in an hour, 3 of each run. 3. For each run, vary the time spacing between each key identification cycle, recording the time between each cycle. Measure voltage and current from the battery to verify it does not go below minimum operating voltage or over maximum current draw of 300mA. 4. After the operation, measure the battery voltage to determine final voltage.
Must stay below 35°.	1. During each run above, also record the peak temperature over the hour.

2.3.2 DC/DC Converter

A converter will be required to manipulate the voltage from the battery to meet the voltage and current requirements of all the individual parts. The RFID reader requires exactly 5 V while the MCU requirements range from 3 to 5 V. Given this, the converter needs one to two outputs to meet the individual requirements. The input will be a 9 V battery, so the converter must be able to step down the voltage over a range of voltages as the battery discharges, from a maximum of 9 V to a minimum of 5.5 V. The converter also needs to allow for the full current draw of at least 300 mA over the range of voltages. Additionally, the converter should not draw from the battery if the battery decreases beyond its minimum value of about 5.5 V and should instead stop operation through undervoltage monitoring.

Requirement	Verification
Must maintain 5 V +/- 5% over a current draw range of 0 mA to 200 mA for each output.	1. For each round of testing, start battery at 100%, 50%, or 10% of full charge. 2. For each port from the converter, measure voltage and current when connected to the RFID reader. 3. During tag reading cycle, record the voltage and current values and for up to 5 seconds after the cycle to observe the full range of voltage output. 4. Repeat this cycle 10 times at each charge level.
Must shut off when supply voltage drops to 5.5 V.	1. To test the shut off capabilities, use a battery at 10% of full charge attach the converter that outputs to a 100 Ω resistor. 2. Measure the voltage of the battery and current flowing to the resistor. 3. Run until the battery hits 5.5 V, monitoring the temperature of the battery to ensure no issues. 4. Converter must shut off before 0.1% further drop of minimum battery voltage, otherwise disconnect circuit manually.

2.3.3 USB Battery Charger

To ensure that the battery is ready to use on consecutive days and with minimum hassle, a charging circuit that pulls from the USB connection is included in the design. This circuit will pull power from the USB when it is connected to the Key Master so the battery can be charged. Charging will occur when the unit is not in use and will charge up to maximum voltage before cutting the current. To ensure that battery safety is observed, the circuit will monitor for overvoltage and overcurrent.

Requirement	Verification
Must pull no more than 1C charging current, or 500 mA, into the battery.	1. Discharge the battery to around 6 V, measuring the voltage for an initial reference. 2. Connect to charger, monitoring current going into the battery is less than 1C. 3. Also monitor voltage over the same charging time, making note when the voltage approaches 5% below maximum charged voltage or about 8 V.
Must cut off current when battery reaches maximum charge voltage of 8.5 V and start feeding current after a 5% drop in voltage.	1. Continuing from the above test, monitor current and voltage. Current should decrease significantly as max charge is approached. 2. At maximum charge, current should cut off immediately. If not, disconnect battery for charging circuit.

	3. Assuming complete current shut off, keep the battery and wait two to three hours for internal discharge to decrease voltage. Verify drop by measuring voltage at each hour mark. 4. At 5% below max voltage, verify the charging circuit starts feeding current again.

2.4 Body

2.4.1 Key Ring Bus

This module will provide a bus that carry the controller's signals and power to the key holders. The ring will have an embedded conductor that will only be in direct contact with the key holders. A protective outer layer will insulate the user against the conductor. The bus will be used for the 1-Wire protocol to send 64 bits serially at a speed of 15.4 kbps, and the protocol consists of 3 phases. The first phase is the reset phase that activates all the chips. The second phase is the select that sends an address to the ROM to select the chip. The third phase is the performance phase of the selected chip where it executes a function, and then the chip loops back to the reset phase.

Requirement	**Verification**
Must maintain its shape with the weight of 10 keys and holders during normal usage.	1. Jostle the ring with the keys on it, wiggle it to ensure the keys have freedom of motion along the axis of the key ring. 2. Remove the keys and measure the dimensions again, noting any specific changes.
Bus contact points must maintain a minimum of 95% voltage from input to the bus after 10,000 connections made.	1. Attach a key to the bus six inches down from the input. Simulate spring loaded contact engaging to the bus 100 times with slight scratching after each contact. 2. Run 5V into the bus input, approximately 6 inches down the bus line with approximately same resistance as 10 keys in parallel. Measure the voltage at input and key locations, as well as bus current. 3. Repeat, measuring voltage down to 4 volts at 0.1 V increments and compare input versus output. 4. Extrapolate a trendline to determine resistance increase and determine degradation after 10,000 connections.

2.4.2 LED Key Holder

This will attach to the head of each key. A hole in the holder's head will facilitate proper contact on the key ring bus while still giving freedom of movement along the ring. Within the holder will be an LED that responds to the signal and utilizes the power to light up the key holder. For design reference, look at Figures 4 and 6.

Requirement	**Verification**
Individually identified addressing works 99% of the time.	

	1. Hookup five of memory elements in parallel to each other. Making sure that the IO pins are all connected to the same bus. 2.Using the microcontroller and the 1-Wire protocol, send a MATCH function down the bus to locate the address.The LED should light up corresponding to the correct address. 3. Run test 100 times, noting how many occasions it fails. For each fail, not the correct address and the identified address.
LED must illuminate at 2.2V or lower voltage.	1. Run the test in a room under standard fluorescent lights. LED should be approximately 2 ft away from viewer and have less than a 45 degree viewing angle.
Must be visible/identifiable in direct sunlight and at a minimum 45 degree angle. The LED's should be visible from at least a yard away. A yard is a good measure because that should cover the longest length of an arm and the ring.	1. Given the turn off voltage, take the LED and power supply so that it is in direct sunlight 2. Starting at a maximum of 5V, slowly decrease the voltage applied to the LED and note when light if no longer visible. 3. Now shut off the lights in the room and decrease voltage until LED is completely off. Note the voltage as turn off.
Must be visible/identifiable in direct sunlight from a distance of 2 ft and at minimum 45 degree angle.	1. Given the turn off voltage, take the LED and power supply so that it is in direct sunlight Again, set up experiment to viewer is about 2 ft away and at least at a 45 degree viewing angle. 2. Starting at the turnoff voltage - 0.5 V, increase the applied voltage until the LED can be easily distinguished as on and ensure the value is below 5 V. 3. Repeat while angling the LED at 30 and 60 degrees and note the point when light is no longer visible at those angles.
Contact with bus must allow for a minimum of 3 V to pass to the key holder.	1. Apply a 5 V variable signal to the keyring bus while 5 key holders are attached in parallel. Send out address signal and verify correct match. 2. Vary the voltage from 5 to 3 V in 0.5 V increments, verify operation of LEDs when an address signal is sent down the bus at each voltage.

2.4.3 Controller Housing

This module will contain all transmission and control elements while doubling as a hand grip. It will connect both ends of the key ring bus, and will also allow for opening and closing of the key ring in order to remove or add keys. The user interface on the housing will have a button to activate the device out of low power operation and read an RFID tag.

Requirement	Verification
Must insulate the user against heat from the battery so that temperature is never above 27°C.	1. With the parts in housing, run key cycles tests in quick succession of 30 seconds on and 30 seconds off. 2. Repeat this cycle 25 times, measuring the temperature of the housing over that time.
Must have a handgrip has a cross section of about 4 in^2 and the extended area to fit in the RFID reader and PCB is least 3"x1'x4".	1. Verify handgrip area by measuring dimensions.
Must weigh less than 0.75 lb. without attached key holders and keys.	1. Weigh the housing after all the parts are inserted into it but without attached keyholders.

2.4.4 User Interface

Consisting of a button and three LEDs, this will allow the user to control when the identification cycle starts and see when it is complete. The button will activate the entire unit such that power is provided to the RFID reader in order to read a chip and begin the process of identifying the correct key. Depression of the button will be required the entire time to run the identification cycle. LEDs will turn on, one to show that the RFID is operating, the second to show that a signal has been sent down the key ring bus, and a third to show a new key has been added. To add a new key, there will be a port in which a new key holder can be inserted for the purposes of identifying the address. While the key is in the port, the RFID reader can be activated to read the RFID tag to be associated with it.

Requirement	Verification
RFID reader only receives power if button is depressed	1. Setup voltmeter at RFID reader input pin. 2. Depress button for time from 1 second to 20 seconds. 3. Check the voltage after button has been released to ensure voltage drops.
LED 1 will turn on while RFID is processing and shut off when RFID is finished with its portion of ID cycle.	1. Connect voltmeter, ammeter at input pin of RFID reader and read voltage in oscilloscope. 2. Hook up LED input to oscilloscope and set trigger for rising edge of RFID input. 3. Start the ID cycle, noting the voltage upon trigger as the LED should turn on shortly after RFID and turn off when RFID voltage drops.
LED 2 will turn on when ID has been made in memory and signal is being sent down key ring bus.	

	Same as above but connect to input of key ring bus rather than RFID 1. LED should turn on only briefly after voltage applied.
Be able to detect if a new key is inserted.	1. Connect two I/O pins of the MCU while using a 1-Wire chip to complete the circuit. 2. Have another I/O pin connected to an LED. 3. Attempt to output a value in one of the I/O pins to the other in the 1-Wire circuit. 4. If a value is detected, have the MCU light the LED. 5. Remove the 1-Wire chip to open the circuit between the two pins. 6. Attempt to output a value of one I/O pin to the other and verify that the LED does not light.

2.5 Schematics

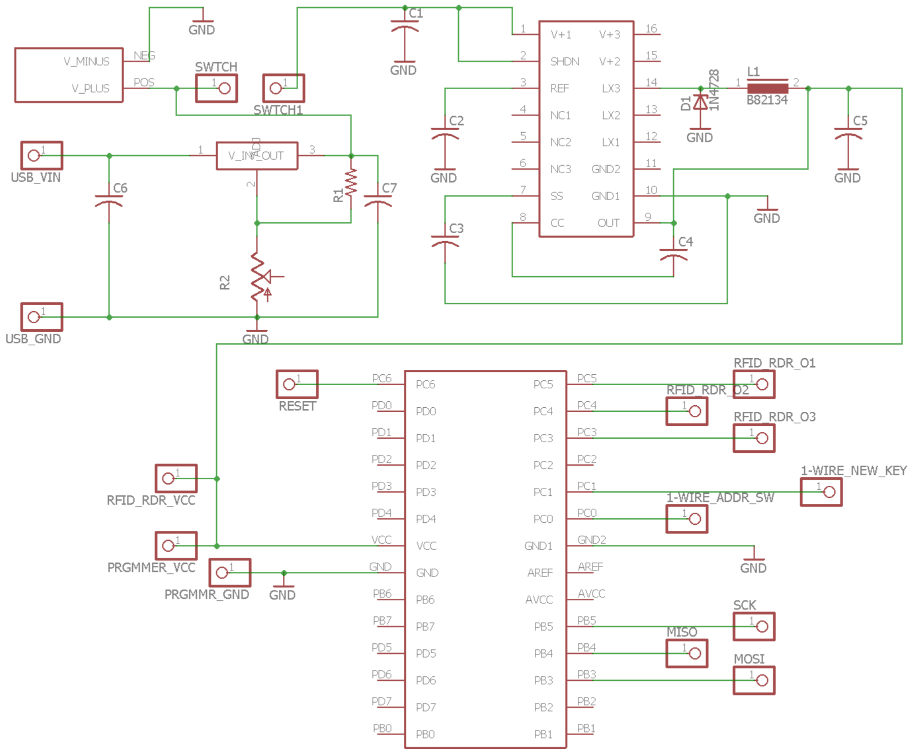

Figure 3: Circuit schematic for the PCB acting as the main hub for parts to connect to.

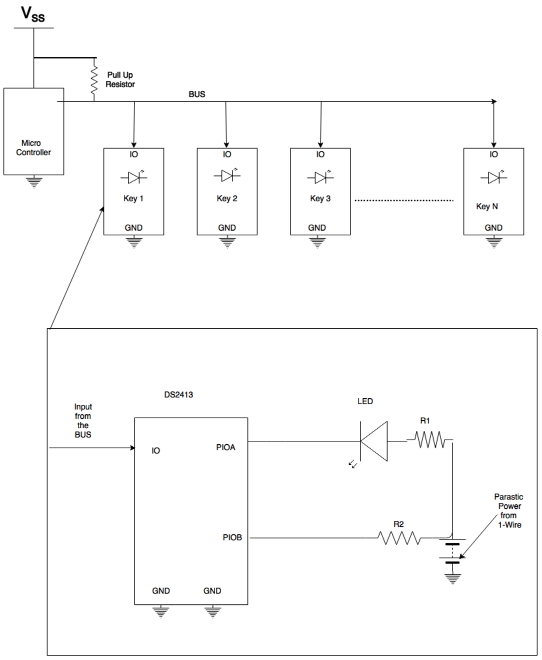

Figure 4: Schematic of the key holder system and for individual keys.

2.6 PCB Design

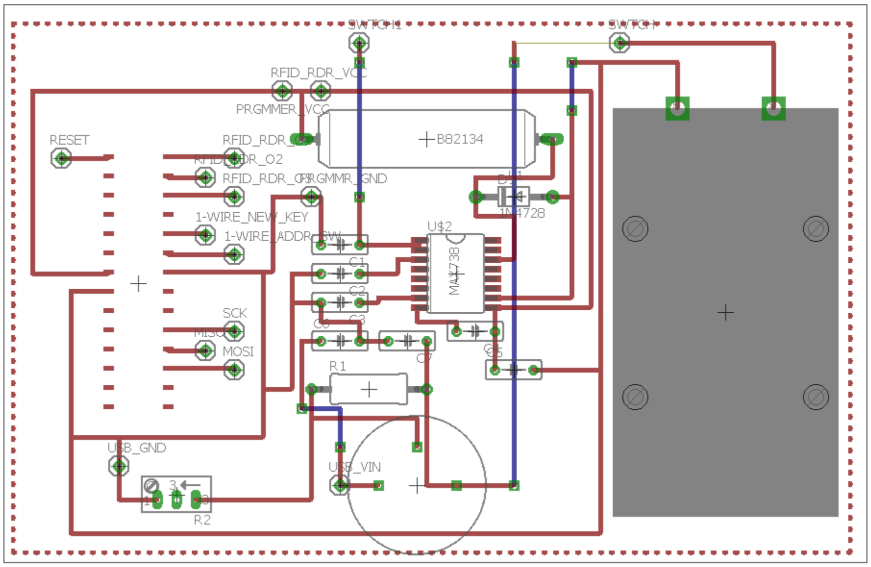

Figure 5: Circuit PCB layout acting as the main hub for component interface.

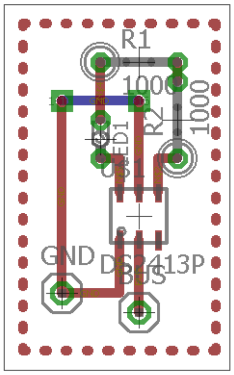

Figure 6: Circuit PCB layout for the key heads.

2.7 State Diagram

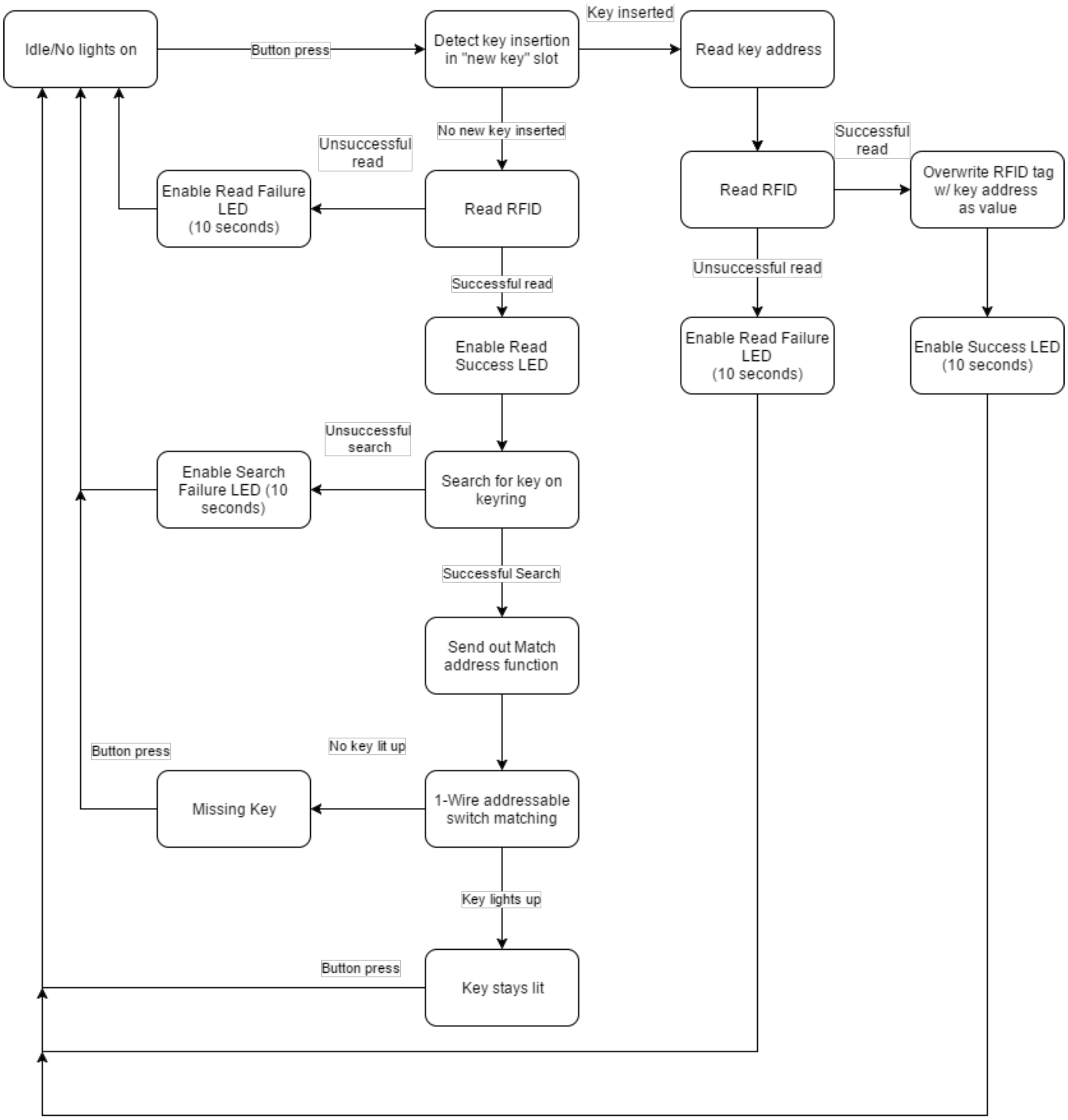
Idle/No lights on
Button press
Detect key insertion in "new key" slot
Key inserted
Read key address
No new key inserted
Unsuccessful read
Enable Read Failure LED (10 seconds)
Read RFID
Successful read
Read RFID
Overwrite RFID tag w/ key address as value
Successful read
Unsuccessful read
Enable Read Success LED
Enable Read Failure LED (10 seconds)
Enable Success LED (10 seconds)
Unsuccessful search
Enable Search Failure LED (10 seconds)
Search for key on keyring
Successful Search
Send out Match address function
Button press
No key lit up
Missing Key
1-Wire addressable switch matching
Key lights up
Button press
Key stays lit

Figure 7: State diagram of Key Master system functions.

3 Tolerance Analysis

The primary failure point in our design is the key ring bus, which will provide a common node points for signal, voltage, and ground lines to all the key holders. The bus will carry all the information needed to identify and light the correct key holder based on the reader. The key holder circuits will have specific voltage requirements in order to convey the signal for identification as well as supply enough voltage to the LED. The current concept for creating contact involve a spring action system of each key's contact points to the buses inside the key ring. For the bus to function correctly, it is required to maintain its shape and keep 95% contact with the engaged key holder nodes for signal and ground buses.

When considering the contact, the main concern becomes the amount of surface area that will be engaged are based on the key holder's external contact points and the bus's ability to maintain over regular application of pressure. Over numerous applications of the spring system, applied force to the bus's conductor material will create indentations that reduce the surface area shared by the key holder contact and the bus. This can be described by the equation (2) given that HBW is Brinell Hardness Number (in kgf/mm2), F is the applied load (kgf), D is the diameter of the keyholder contact (in mm), and d is the diameter of the indentation in the bus (in mm).

$$\mathrm{HBW} = 0.102\frac{2F}{\pi D(D - \sqrt{D^2 - d^2})} \tag{2}$$

$$\begin{aligned} \mathrm{d} &= \sqrt{D^2 - (D - \tfrac{2F}{\pi \mathrm{D\ HBW}})^2} \\ \mathrm{d} &= \sqrt{0.9398^2 - (0.9398 - \tfrac{2*0.03}{\pi*0.9398*35})^2} = 0.03303 \text{ mm} \end{aligned}$$

Working with copper contact wires from the keyholder of 20 AWG gives a indenter diameter of 0.9389 mm. The approximate applied load is about 30 g for the key and key holder, resulting in at most a force of 0.03 kgf. The hardness for copper is 35 kgf/mm^2, resulting in a calculated indention of 0.03303 mm. Indentation size in the bus can be used for a number of effects that our bus must overcome to ensure reliable operation. The indentation can be used as an initial estimate of the increase in resistance due to a loss of surface area contact, though over a number of . Either form of added resistance, increasing over time, will degrade the signal and voltage sent across the systems. Given 100 reads expected daily, and up to 26,000 a year, the number of cycles could shortly render the bus ineffective with higher levels of wear on the contacts.

Translating the initial loss in conductivity comes down to determining resistance per meter. Given copper's resistivity is 1.72*10^{-8} $\Omega \cdot$ m, the starting resistance for the key ring bus will be around 0.0.332 $\Omega \cdot$ m. After one contact cycle and indentation, the increase in resistance due to loss in surface area is found below:

$$\begin{aligned} \mathrm{R} &= \frac{\rho}{\Delta A} \\ \mathrm{R} &= \frac{1.72*10^{-8}}{\pi \frac{((0.9398-0.03303)*10^{-3})^2}{4}} = 0.0266\Omega\cdot \text{ m} \end{aligned}$$

Cycling through the repeat process of 26,000 cycles will increase the size of the indentation, along with some wear and tear loss to the key holder contact will continual decrease the surface area of the contact. This sort of repetition has shown a fairly linear relationship until it saturates, with approximately a 6 fold increase in area over 30,000 cycles though tested cases were dealing with vibrations at 10 Hz than our system. [7] The contact frequency for the Key Master is much less than this, but the number of occurrences will add up. Using the 6 fold increase in area as a maximum in this case, the resistance would only increase to 0.0398 $\Omega \cdot$ m. This also does not account for potential loss in contact effectiveness due to air gaps or corrosion of the partially exposed bus. [6] There is the potential for signal erosion due to to these factors as well, however testing will be required to ensure the bus. Assuming the initial contact variance in resistance is as low as calculated, then voltage should be almost entirely maintained.

This bus will have to be made correctly in order to transport our signal without causing harm to the user or failure of identifying the right key. If the keys are not touching the bus, then they can not be identified correctly. The bus should be built in a way that all the keys make contact with the bus and are capable of reading the incoming signal from the hand grip. A larger portion of the risk associated with this design is the safety of the user of the device. If the bus is exposed, it could potentially make contact with the user can cause major harm. The bus needs to be properly shield so that accidental contact to the live wire is impossible.

4 Cost and Schedule

Labor will account for the largest chunk of expenses in completing this project. Given an above average salary for UIUC graduates of approximately \$72,000 plus benefits of \$6,000, we can estimate an hourly rate of

$$\frac{78{,}000}{40 \text{ hours per week}} \times \text{ 52 weeks} \quad = \$37.50$$

$$3 \times \$\ 37.50 \times 10\frac{\text{hr}}{week} \times 16\text{weeks} \times 2.5 \quad = \$45{,}000$$

Work on this project is expected to be about 10 hours a week per person for 16 weeks to complete the prototype with additional expenses for equipment and workspace cost at 2.5 of the total.

Additional costs for housing is estimated at \$50 with machining labor of 20 hours of labor at \$25/hour and 5 hours of machining at \$50/hour. Machine shop costs total at \$800. Including all parts, labor, and etc. costs is a grand total of \$45953.94.

Table 5: Schedule

Week	**Petar**	**Amanda**	**Leslie**
2/6/2017	Design key holder identification circuit per individual addressing.	Calculate power needs based on initial part requirements.	Research MCU options and confirm memory size for max key of 100 count.
2/13/2017	Research signal processing options for identifying individual keys.	Research part options and design for charging and conversion circuit.	RLC circuit testing and test RFID reader from the lab.
2/20/2017	Design Review: circuit schematics and parts research.	Design Review: power calculations and tolerance analysis.	Design Review: PCB design and document organization.
2/27/2017	Simulate key holder circuit and order parts.	Order power parts, finalize dimensions with machine shop for housing.	Order MCU, programmer and research code.
3/6/2017	Test the RFID reader and determine the read ranges when the reader has plastic between it and tag.	Model and test bus contact erosion to determine resistance increase and voltage drop from repeat use.	Begin coding the protocols into the microcontroller for the key ring holders.
3/13/2017	Test a key holder circuit on breadboard.	Simulate longer term erosion of bus contacts, breadboard battery charging circuit.	Finish protocol for identifying keys and match to specific RFIDs. Breadboard unit testing.
3/20/2017	Test key holders in parallel, sending out data bits to confirm address verification using Arduino.	Debug battery charging circuit. Order the keyholder and controller PCBs.	Test the code onto the breadboard key holders.
3/27/2017	Place the PCB's on the holder and attach test keys. Attach to Bus.	Submit key holder circuits to machine shop for inclusion in fabrication.	Debugging the code for the transmitter. Test the output of the microcontroller.
4/3/2017	Verify that the tags can read by the reader and output the keys.	Test key holders to ensure they respond in holder.	Test adding new keys to the system.
4/10/2017	Test how many times the device fails in identifying the right keys.	Attach key holder to key ring bus. Test contact and debug.	Test modular function.
4/17/2017	Continue testing the reader and key holders.	Continue testing bus with more keys added on.	Continue testing with keys not in system to see if will not be identified.
4/24/2017	Place PCB in housing and test.	Debug remaining problems.	Debug remaining problems.
5/5/2017	Demo.	Demo.	Demo.

Table 6: Parts and Costs

Part	Quantity	Cost (per unit)	Cost (bulk)	Cost (total)
Sparkfun Pocket AVR Programmer	1	$14.95	$14.95	$14.95
9V Rechargeable Li-Ion Battery (Batterymart R-LI9600)	1	$11.95	$10.95	$11.95
ATMEGA8-16PU Microcontroller	1	$2.48	$2.06	$2.48
Parallax RFID Read/Write Module (Jameco, 2123514)	1	$49.95	$49.95	$49.95
Yellow LED 1000mcd (DigiKey, 754-1889-ND)	10	$0.546	$0.21	$5.46
DC/DC converter (DigiKey, MAX738ACWE+-ND)	1	$4.32	$3.70	$4.32
Charger IC (Digikey 296-35898-ND)	1	$13.26	$8.39	$8.39
RFID tags (Nextwarehouse, 32399)	10	$3.14	$3.14	$31.40
Button (Mouser, 510PB-ND)	1	$0.89	$0.89	$0.89
Battery Holder (Mouser, 534-1294)	1	$1.94	$1.15	$1.94
1-Wire Dual Channel Addressable Switch (DS2413, Maxim Integrated)	10	$2.67	$1.71	$26.78
Capacitor 1.8 uF (KEMET, C1210C185K3RACTU)	1	$0.81	$0.81	$0.81
Capacitor 6.875 uF (Murata Electronics North America, GRM155R71H103KA88D)	1	$0.10	$0.10	$0.10
				$164.29

5 Safety and Ethics

After reviewing the IEEE and ACM code of ethics, it is safe to say that our project will follow the entirety of the code of ethics with special attention required for the code says to not purposefully create something that will do harm [3] [4]. The project will need to specifically pay attention to any power sources and any exposed conductors to ensure it will not cause any damage to the user or others without purposefully bypassing safety designs.

The key system involves a semi exposed conductor that will need an adequate design to ensure user and bystander safety. Warning labels will be needed on the physical device to notify the user of the conductor, and instructions should be included to state the intended usage and environment for the system. These instructions should also clearly state what to avoid with the system to ensure user safety.

The conductor needs to be enclosed as much as possible for the safety of the user and others so that the conductor can only be touched with a tool. The enclosure would be a thick, non-conductive material with a thin slit for the key housing to reach the conductor but not thick enough for a fingertip to reach through.

This product requires portability, meaning the power source needs to be small but have a high capacity. Batteries in general have some inherent dangers that require proper handling and storage. It is important to provide short circuit protection for any battery, no matter the chemistry. When a battery is shorted, currents of values higher than rated discharge current can be produced which will overheat the battery and may even cause it to ignite.Including a fuse that will break current flow above a certain value will help protect the user in the event of a short.

A lithium ion battery will be in use for this design, so there are a number of additional precautions that need to be taken as to remove chances of failure. The chemical composition of lithium ion makes them the best way to minimize the size of portable devices while maintaining the highest capacity, but are also much more flammable than other battery compositions. Their operating range is limited by specific values of over and under voltage, as well as maximum charging currents. In order to address these concerns, ICs will be used to ensure that, if the battery discharges to its minimum, the circuit will break and cease operations.

Charging will require the overvoltage and overcurrent monitoring. As the battery's charge approaches the maximum, the current should decrease significantly, to be controlled based on maximum voltage of the battery. There will also be an IC controlling a complete shut off of the charging circuit when at maximum and allow the charging to begin again when the voltage has degraded to below 5%. By controlling the flow of charging, this ensures that the battery remains within its limits and will not overheat.

The user will not have direct contact with the battery as it will be completely be encased in the controller housing/handle. This should minimize any physical damage that could affect the battery. Any lithium ion battery should be removed if it becomes dented, so the user will need to check the battery if the unit has been dropped from from a height of above 2 ft. Additionally the user should be cognizant of the temperature of the housing, which is indicative of potential issues that regarding current and voltage.

The user should hold the grip/controller if not attached to their person. The key ring should be touched only when necessary, such as retrieving a key from the ring. The user must avoid gripping the key ring along the slit to minimize potential of a shock. If the user's hand is wet, do not use the system until dry.

The intended environment is for a dry, clean location with little sources of exposed liquids or fine particles that can deposit in the slit. Care is necessary when handling the system in a moist and/or dirty environment. If the slit needs to be cleared, the system should not be in use and have its power source disconnected before attempting. A fuse will be included along the exposed conductor's connection in order to prevent too much current drawn.

6 References

[1] Stanley Security Solutions, "BEST Price List 60 GSA," in Stanley Security Solutions, 2011. [Online]. Available: http://www.stanleysecuritysolutions.com/files/documents/GSA%2060%20Best.pdf. Accessed: Feb. 9, 2017.

[2] USB Implementers Forum Inc., "USB 2.0 documents," in USB.org, 2012, sec. USB 2.0 ECN VBUS Max Limit. [Online]. Available: http://www.usb.org/developers/docs/usb20_docs/. Accessed: Feb. 9, 2017.

[3] IEEE, "IEEE code of ethics," in IEEE, 2017. [Online]. Available: http://www.ieee.org/about/corporate/governance/p7-8.html. Accessed: Feb. 9, 2017.

[4] ACM, "ACM code of ethics and professional conduct," in ACM, 1992. [Online]. Available: https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct. Accessed: Feb. 9, 2017.

[5] Friction and Friction Coefficients [Online]. Available: http://www.engineeringtoolbox.com/friction-coefficients-d_778.html. (2017, February 15). List of Copper Alloys [Online]. Available: https://en.wikipedia.org/wiki/List_of_copper_alloys

[6] Nuruzzaman, D.M. and Chowdhury, M. A. (2012, November 1). Friction Coefficient and Wear Rate of Copper and Aluminum Sliding Against Mild Steel. [Online]. Available:http://tuengr.com/V04/029-040.pdf.

[7] Park, Y.W., Sankara, T. S., and Lee, K.Y. (2006, October 24). Fretting Wear Behavior of Tin Plated Contacts: Influence on Contact Resistance [Online]. Available: (http://www.academia.edu/2922746/Fretting_wear_behaviour_of_Tin_plated_contacts_Influence_on_contact_resistance. Common Wire Gauges [Online]. Available: http://hyperphysics.phy-astr.gsu.edu/hbase/Tables/wirega.html.