Key Master

RFID Based Key Choosing System

"These keys are lit."

Team 14

Team Members:
Petar Barac
Amanda Beck
Leslie Cheng

TA:
Jacob Bryan

February 7, 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 larger numbers of keys, navigating buildings can be difficult to navigate efficiently because of the numerous locks in place that may require an equally large number of keys unless a master key exists. Unfamiliarity with the building and keys also causes efficiency problems when opening a door involves trial and error. The more keys involved, the longer this process will take especially if multiple locks are accessed. 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.

Electronic locks help with this problem because one keycard can open all the locks, but this might not be an option for older buildings with physical locks since all the locks would need to be powered and replacing every physical lock would be expensive (over $1000 per lock for those in the ECEB [1]). Such a lock would also be meant 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

- The system has to be able to reliably read an RFID tag within a distance of approximately 10 cm.
- Once a RFID tag has been read, the system has to be able to light up the correct LED of the key associated with the tag/lock.
- A good battery life is needed so that the system can be used multiple times, approximately 12 times, within a standard 8 hour work day.

2 Design

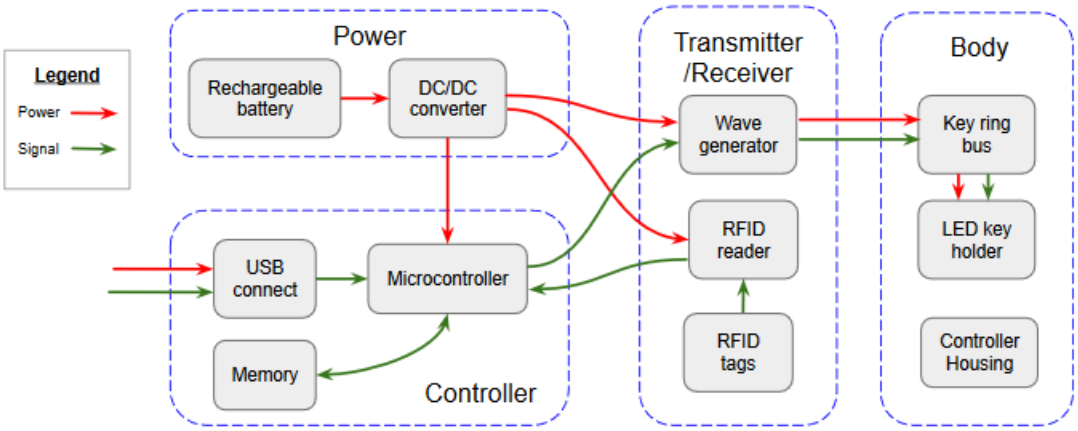

Figure 1: Block diagram of Key Master components.

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.

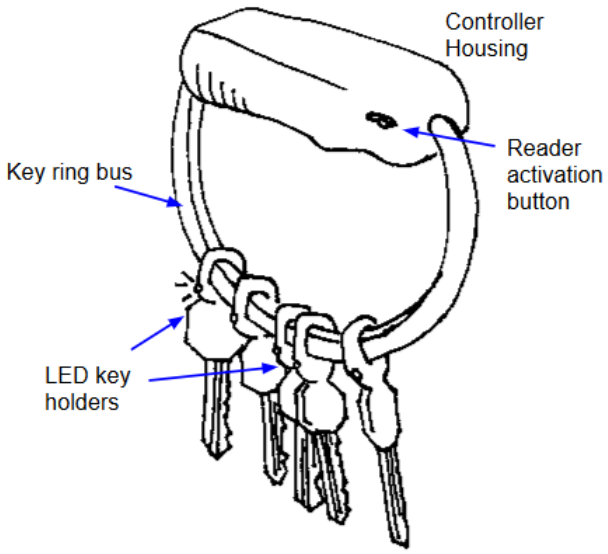

Figure 2: Sketch of the intended physical design of the system.

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 signalling the user.

2.1 Controller

The controller module is responsible for storing the frequency values associated with each RFID tag. It receives an input from the reader, and then it will automatically lookup the value in memory and output the frequency value to the transmitter.

2.1.1 Microcontroller Unit

The microcontroller unit 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 frequency needed to resonate with the key. This frequency is then sent out to the wave generator so it can output the frequency through the keyring.

Requirement 1: Must run between 4.5V to 5.5V and draw less than 500 mA as the peak current.
Requirement 2: Be able to receive and output at least 16 bits.
Requirement 3: Has to be programmable and independently produce an output after receiving an input due to the programming.
Requirement 4: Program must be retained even after power has been shut off.

2.1.2 Memory

The memory will contain all the frequencies needed for the keys and the RFID information will be used to lookup the frequencies. There should also be a self contained power unit included with the memory so that no information is lost if the main battery to the system is disconnected, and the memory does not drain as much power. The internal power unit will charge at the same time the main battery would to minimize overall power draw.

Memory receives all its inputs from the microcontroller and outputs to it as well because it only serves as a table of values. The size of the memory does not need to be very large as well because the limiting factor of how many values will be stored is the amount of keys that can fit on the keyring. Ideally the memory unit is already integrated into the microcontroller for our purposes.

Requirement 1: Must run between 4.5V to 5.5V and draw less than 250 mA as the peak current.
Requirement 2: Be able to receive and output at least 16 bits.
Requirement 3: Stored values must be retained after power has been disconnected.

2.1.3 USB Connect

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].

Requirement 1: Must follow standard USB specs (between 4.75V to 5.25V and up to 500 mA for input).
Requirement 2: USB port must be Micro-B format.

2.2 Transmitter/Receiver

This module is responsible for reading RF inputs to be processed by the control unit. It is also responsible for submitting the matched output as a pulsed signal to a key frequency.

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. The tags should be purely passive, and draw no power.

Requirement 1: Must be unique and not have identical information of another tag.
Requirement 2: The tag must be able to be read by the reader from at least 5 cm away.

2.2.2 Wave Generator

The wave generator is the component of this project that will provide approximately 0.8V at specific frequencies within the MHz range so that they can power only one resonant key at a time without interfering with the neighboring keys. (Each key will have a specific frequency)

Requirement 1: VCO must be able to provide approximately 0.8 V across a frequency range of 800 MHz to 1 GHz.
Requirement 2: The frequency output should have a bandwidth that is less than the difference of two resonant frequencies of the LED Key Holder

2.2.3 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 1: The reader must be matched to 50 Ω and have a read range of at least 5 cm. It should be able to operate it on 5 volts.
Requirement 2: Must be easy to carry.

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 9V battery will serve. This should be sufficiently large to power all the elements while also being compact enough to fit in a handgrip-sized housing attached to the key ring.

Requirement 1: Must provide at least 500mAh at 9V for a minute and stay below 35°.
Requirement 2: Must last for at least eight hours with up to a dozen RFID reads.

2.3.2 DC/DC Converter

A converter will be required to step down the power given from the 9V battery. The MCU, USB port, and RFID reader will require around 5V, and will need consistent voltage.

Requirement 1: Must maintain 5V +/- 10% over a current draw range of 20 mA to 500 mA

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.

Requirement 1: Has to be large enough to fit at least 10 keys.
Requirement 2: Must maintain its shape with the weight of 10 keys and holders during normal usage.

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.

Requirement 1: Must illuminate at 2.2V or lower voltage.
Requirement 2: Must be visible/identifiable in direct sunlight.

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 1: Must insulate the user against any heat from the battery and other modules.

3 Risk Analysis

The RFID reader is extremely vital to being able to successfully use the Key Master. This antenna is what allows us to identify the RFID tags on each lock, and it must correctly read the tag in order for the appropriate key to be used. The range of the reader should be no larger than 5 cm to ensure that other nearby tags are mistakenly identified by the reader. The RFID reader will not be built from scrap, but we will use an existing reader and integrate it into our design. The integration of the reader will require us to make sure that it's impedance is matched to 50 Ohms. Matching allows us to get the maximum power out of our reader which is vital if it is desired to keep power consumption as low as possible. It is also important to make sure that our reader is following all FCC regulations and does not interfere with other existing technologies. Another major consideration that needs to be taken account of when working with our reader is the electromagnetic output. There are specific limits that are allowed and optimal from our specific uses.

4 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.

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.

5 References

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.