RFID Tunnel Project Report

A system for extending the range of RFID over a distance.

MIT 6.101 – Analog Electronics Laboratory
Spring 2014

Vineel Adusumilli
Austin Duffield
Brandon Vasquez

Abstract

In this report, we describe a method for tunneling 125KHz RFID tags over a distance. We deal explicitly with tunneling amplitude-shift keying RFID tags, and propose a method for tunneling the phase-shift keying tags that are commonly used for security purposes.

Table of Contents

List of Figures

Introduction

Overview

The RFID Tunnel project is meant to demonstrate a fundamental security flaw in RFID: readers have no way of verifying that the tag is physically present. To demonstrate this a system was designed to trick readers into believing they are reading a tag that is far outside the range of the reader.

The RFID Tunnel relays an RFID signal over a considerable distance by acting as a bridge between an RFID card and an RFID reader, specifically using 125KHz cards and readers. There are two distinct physical devices: a reader emulator and a card emulator. The reader emulator is be placed near a card, exciting it and sending any output data over an RF link to the card emulator, which is placed near a reader. The card emulator then conveys the received information to the actual reader. Both the reader emulator and card emulator are designed to be low power and portable, yet still able to transmit a signal over a reasonable distance.

System Breakdown

The main goal of this project was to implement one way communication between an RFID card and reader. The critical path is denoted using the solid lines. A possible extension to this project is denoted using the dotted lines. This extension would be to implement two way communication, bringing on new challenges such as using two different transmission frequencies and detecting when to receive and transmit data for RFID systems that use a handshake.

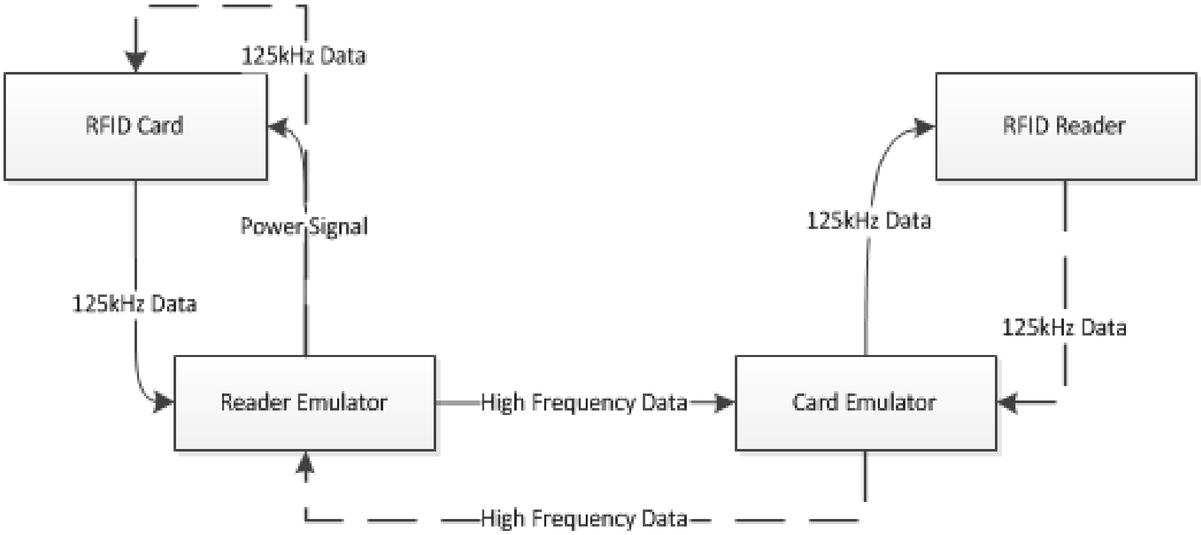


Figure 1: System block diagram

RFID Overview *by Vineel Adusumilli*

Radio-frequency Identification (abbreviated RFID) is a technology that has existed for decades. The original purpose was to track goods, animals, or other materials. Nowadays, it is also used for security purposes such as access control or paying tolls and fares.

RFID systems are composed of two components: a tag and a reader. Readers excite tags using an RF field generated by an antenna coil. The tag then selectively reflects or attenuates the signal in order to convey data. Most RFID systems in use today are passive, meaning that the tags don't contain a power source and are entirely powered by the RF output of the reader.

There are three methods of conveying information over RFID: frequency-shift keying, amplitude-shift keying, and phase-shift keying. This final project dealt explicitly with the latter two methods, and would likely work with the first with minimal or no modification.

Amplitude-shift keying works by selectively attenuating the RFID carrier frequency. In the case of our project, this frequency is 125KHz. When the carrier is attenuated, the value conveyed is a digital one. When the carrier is unattenuated, the value conveyed is a digital zero.

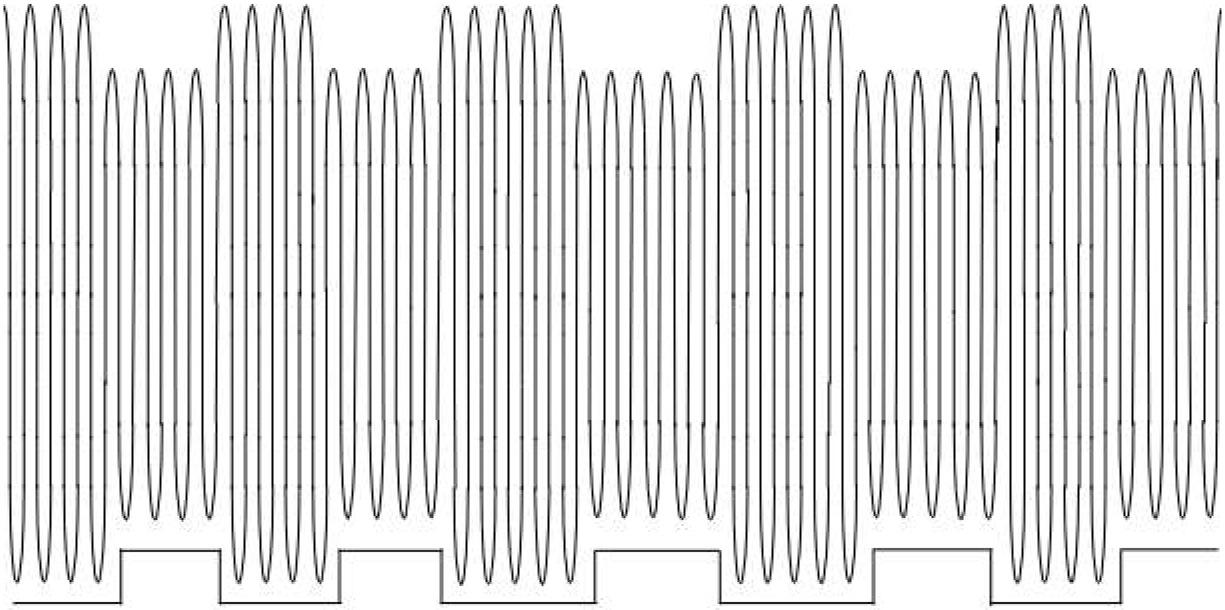


Figure 2: Amplitude-shift Keying (Source: Microchip)

Frequency-shift keying works in a similar manner: the tag switches between two frequencies, one meant to represent a one, and the other meant to represent a zero. Due to selectivity of the reader coil, one of the frequencies is attenuated more than the other, creating a result that is nearly indistinguishable from the amplitude-shift keying shown above. This is why we believe our system would also work well with tags that make use of frequency-shift keying. The majority of cheap, commercial RFID readers on the market are ASK/FSK readers.

Phase-shift keying is much more complicated, but supports a higher data transfer rate: up to half of the carrier frequency (62.5KHz in the case of MIT IDs). It works by switching control of the attenuation of the carrier between two square waves that are half of the carrier frequency and exactly out of phase with each other. The phase shift boundaries denote whether the information conveyed is a one or a zero. [1]

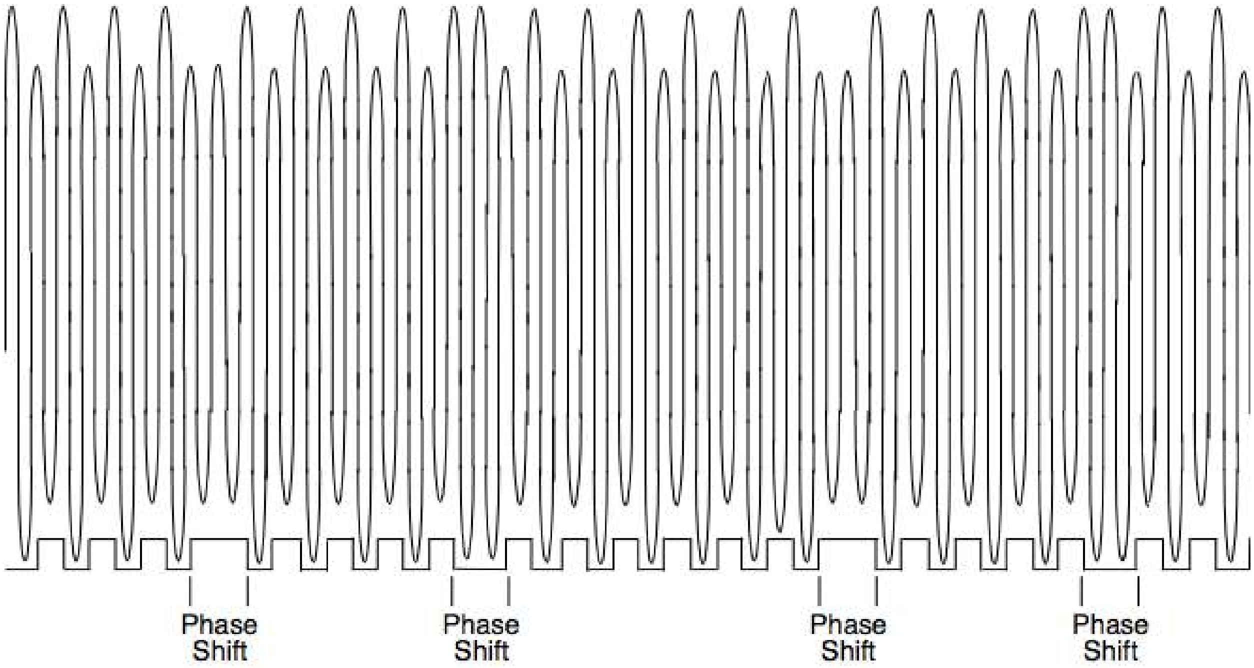


Figure 3: Phase-shift Keying (Source: Microchip)

Design

Reader Emulator *by Brandon Vasquez*

The reader emulator has four major stages: 1) 125KHz signal generator, 2) RF amplifier 3) Sharp 62.5KHz filter and 4) Peak detection. The 125KHz signal generator was accomplished using a 555 in an astable configuration with a potentiometer for fine adjustments. The 125KHz signal was used to drive the RF amp, a bjt push-pull driver. This amp was used to drive the resonant LC circuit which would transfer power to the card. The 2N2222 and 2N2907 were used for the high and low bjts. Two diodes were used to compensate for cross-over distortion which was not entirely necessary since the input signal was 0-5V square wave from the 555. A 470Ω resistor was used to limit the current into the bjts while 10Ω resistors were placed on the emitters to increase stability.

The push pull driver drives a series LC circuit which was designed to resonate around 125KHz. A series LC circuit was used instead of a parallel one to maximize the current through the coil, which results in more efficient energy transfer to the card. The coil, which was constructed using 22 gauge magnet wire and 80 turns, achieved an inductance of approximately 1.2mH at 125kHz. The dimensions of the rectangular coil were about 10cm x 8cm. A capacitance of 1.5nF was calculated to cause resonance with the coil so a 1.3nF and 200pF cap were used.

The output of the LC circuit was AC coupled through a 1uF cap to an envelope detector which consisted of two diodes, a 1MΩ resistor, and a 1nF cap. This portion of the circuit is used to detect the envelope of the 125Khz carrier frequency which is the 62.5Khz signal frequency. The 62.5 KHz signal is then sent through an AC coupling cap and added to a DC voltage of around 1.2V which is set by 100KΩ and 330KΩ resistors. This now DC biased signal is put through a 3-pole filter created with a LC low pass filter and a sallen-key filter. The resistors and capacitors were chosen to create a sharp filter at 62.5KHz.

The output of the filter was AC coupled again and given a DC bias voltage of 2.5V. It was then gained by 11 through an op-amp with a virtual ground of 2.5V. This virtual ground was created with a resistor divider and buffered by an op-amp. The last stage of the Reader Emulator involved a voltage comparator with hysteresis. The threshold levels were chosen to pick up the peaks of the 62.5KHz signal and turn them into a digital signal. Each phase transition would result in a peak which would be translated into a high or low given the direction of the peak. This makes transferring the data from the Reader Emulator to the Card Emulator easier and more immune to noise.

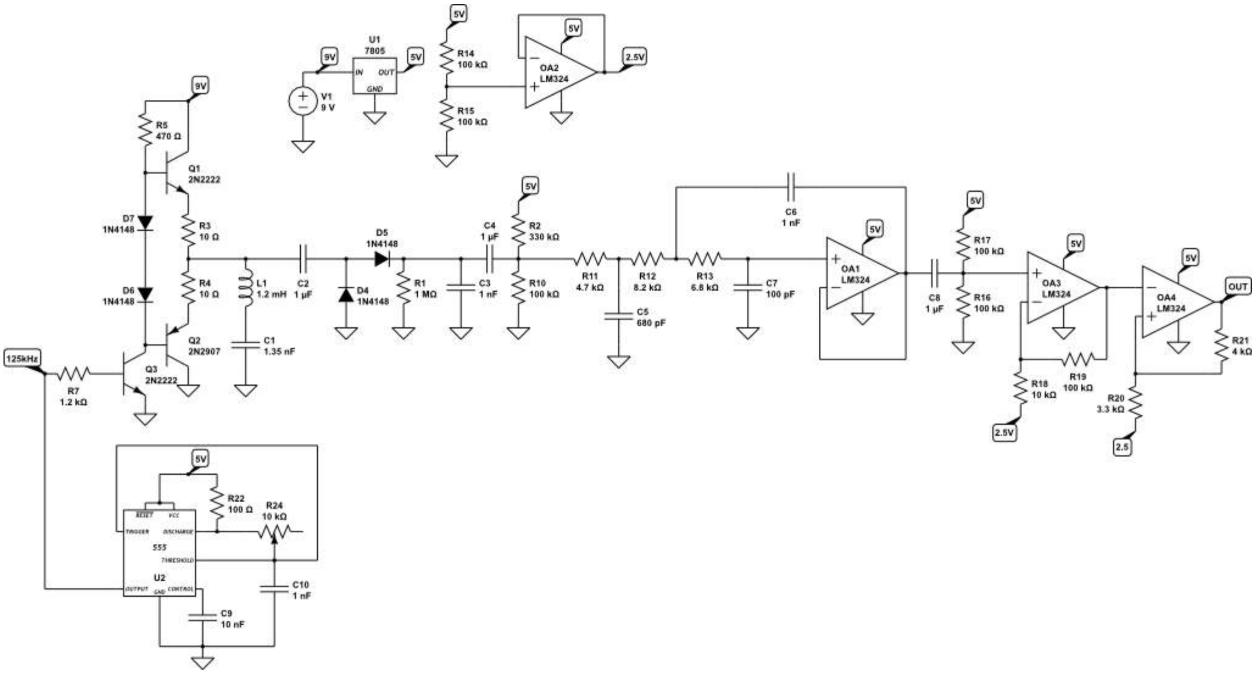


Figure 4: Reader Emulator Schematics

Card Emulator *by Vineel Adusumilli*

The amplitude-shift keying card emulator turns out to be a fairly simple design. Unfortunately, we were not able to get the frequency-shift keying emulator working (more details are provided in the Discussion section).

The schematics for the amplitude-shift keying card emulator are as follows:

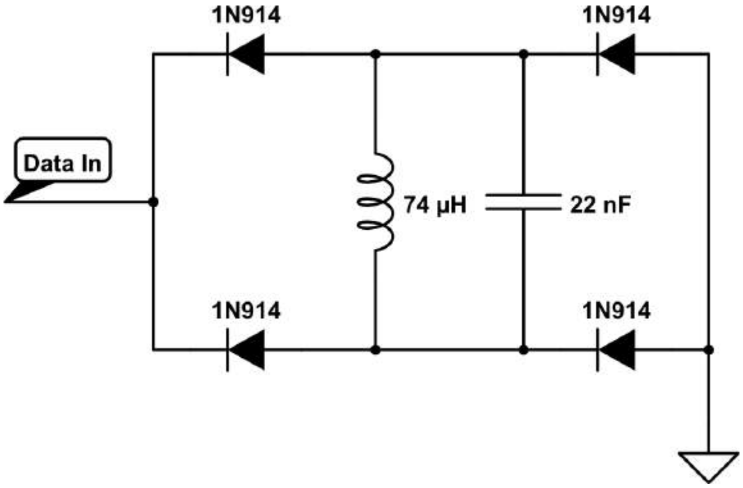


Figure 5: Card Emulator Schematics

The 74µH inductor is a custom-wound coil made out of magnet wire. It is matched with a 22nF capacitor in order to create a resonant tank that resonates at a frequency very close to the 125KHz operating frequency of our RFID system.

The "Data In" node is a digital signal coming from the reader emulator and through the RF link. When the signal is low, the diode bridge acts to attenuate the signal across the coil. When the signal is high, the diode bridge has no effect, leaving the carrier unattenuated.

RF Transmission *by Austin Duffield*

The radio transmitter and receiver operate at 25.125MHz using simple on-off modulation with carrier detection. The transmitter uses an excited crystal to achieve the desired carrier signal, appropriately filtered to remove harmonics and achieve a clean sine wave. This is then coupled to the base of a 2n2222 bjt for amplification. The amplified signal is then passed through a simple LC matching network into a simple 12” wire antenna. The capacitance is tuned for best power transmission into the antenna.

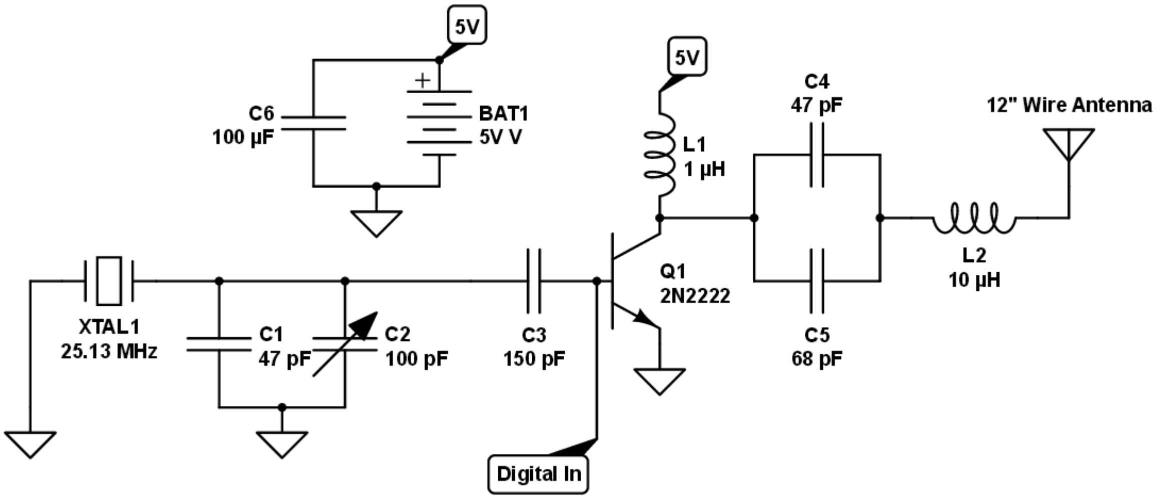


Figure 6: Transmitter Schematics

A typical regenerative receiver topology is used to pick up the signal at a distance. The same 12” wire antenna is used, easily coupling with the transmit antenna at a distance of more than ten feet. A simple LC tank circuit tunes the receiver to the 25MHz carrier. The resulting signal is low-pass filtered to remove the carrier. Because the signal is on-off modulated, the result of the low-pass is either a high or a low, indicating the presence or absence of the carrier. This is passed to two gain stages, also using 2n2222’s, which serve to clean up the signal and deliver 5V railed voltage levels for a digital output.

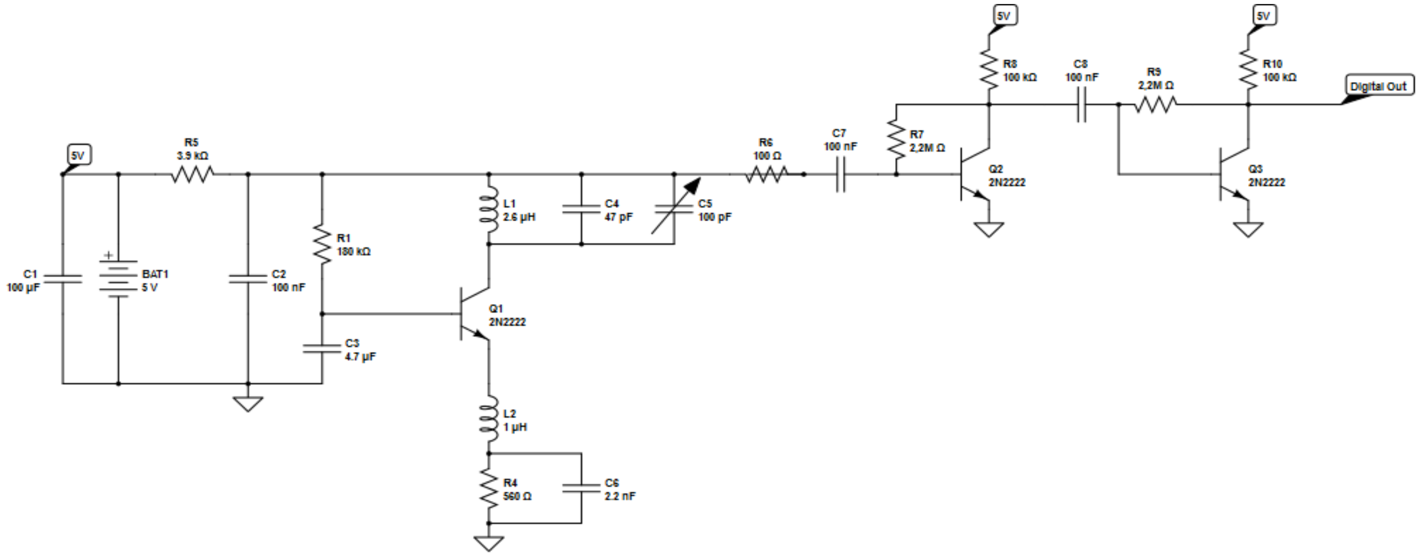
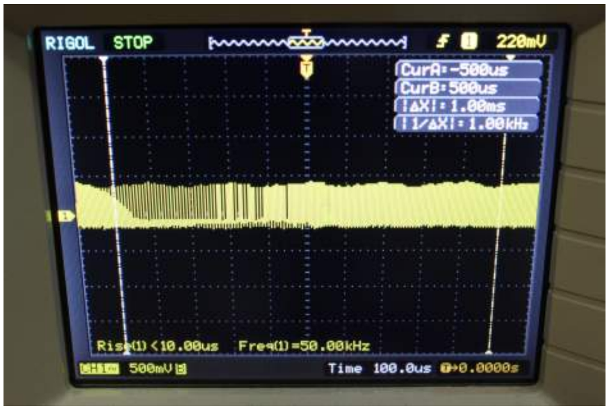


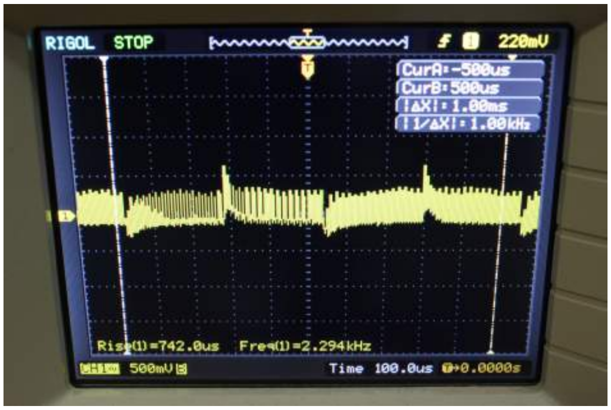
Figure 7: Receiver Schematics

One complication in the implementation is the inductors in the tuning circuits of both the transmitter and receiver. In order to avoid core losses and strange behavior at high frequency, these were implemented as hand-wound air core inductors. The inductance was roughly calculated using the standard formula L= (d^2 * n^2)/(18d+40l), and then tuned using a variable-frequency LCR meter.

Testing

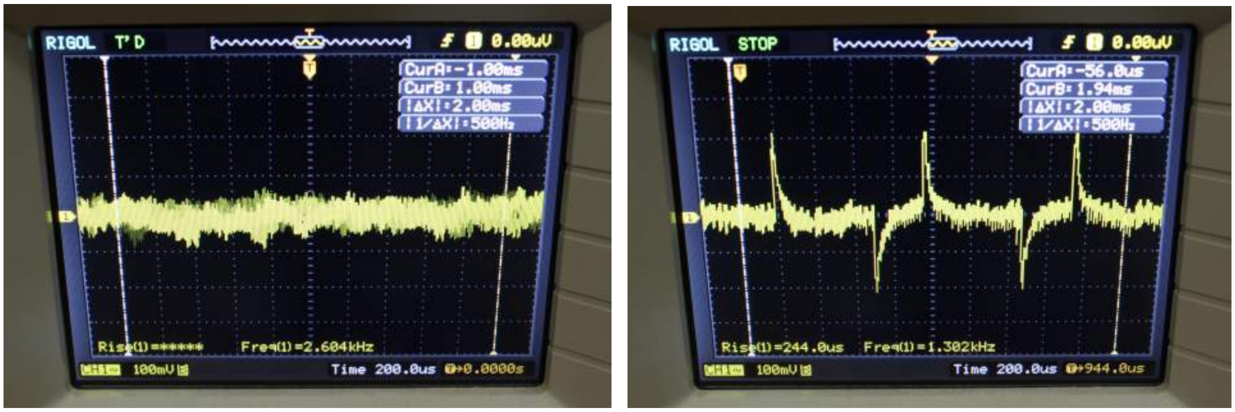
To test the Reader Emulator, various points along the signal path were scoped. To check if the MIT RFID cards were being excited, the output of the envelope detector was observed. Without the presence of a 125KHz RFID card, the output was expected to be relatively constant. In the presence of a card, noticeable spikes in the RFID signal can be observed, which signify attenuation of the 125KHz signal by the card.





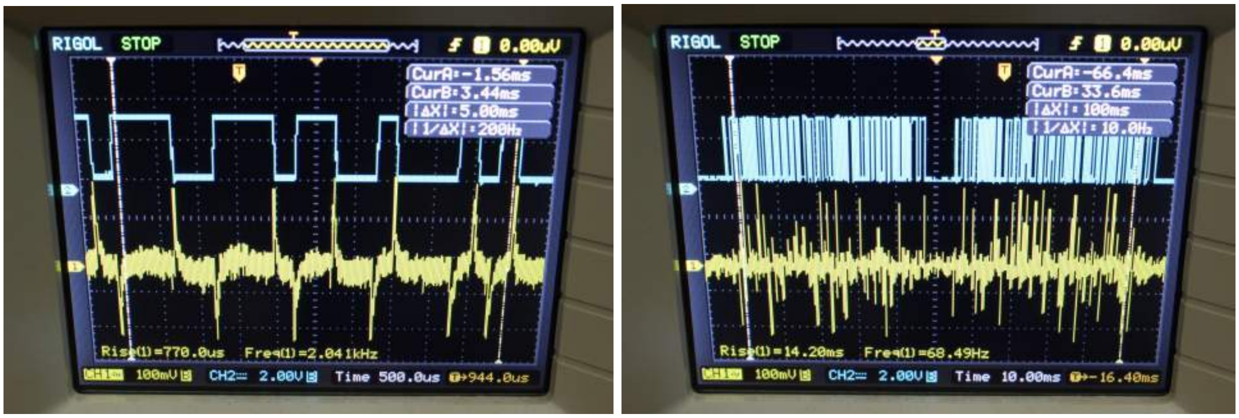
Figures 8 and 9: The figure on the left is the output of the envelope detector in the absence of an MIT RFID card (vertical scale 500mV). The right figure is with an MIT RFID card within range of the antenna (same vertical scale).

After applying the filter, significant reduction in the amplitude of noise can be seen compared to the signal.



Figures 10 and 11: The figure on the left is the output of the 3-pole filter in the absence of an MIT RFID card (vertical scale 100mV). The figure on the right is with an MIT RFID card within range of the antenna (same scale)

Lastly, to check if the final gain stage and comparator is working, the signal on the output of the filter was compared to that of the comparator.



Figures 12 and 13: The figure on the left is the output of the filter (yellow) compared to the output of the comparator (blue). The figure on the right is a longer capture of the data sent by the card.

Each phase change results in a change in the digital signal which can be observed in the figures above. The figure on the right demonstrates the repetitive signal sent by the MIT RFID card.

Unfortunately, the type of RFID reader necessary to read an MIT ID card is prohibitively expensive, so we had no effective method of testing our tunneling system outside of walking to the nearest reader after every tweak. This made iteration difficult. We ended up testing the tunnel using 125KHz amplitude-shift keying tags and a cheap RFID reader sourced from eBay.

We had two distinct RFID tags. Each one, when presented to the reader, would cause it to display a unique number on the computer it was connected to. We set up the tunnel by presenting the card emulator to the reader, and the tags to the reader emulator. When we did this, the same unique numbers would show up as when we presented the tags directly to the reader.

Discussion *by Vineel Adusumilli*

The original goal of this project was to tunnel MIT ID cards. This proved to be a fairly difficult task. The only concrete information available on MIT ID cards was a paper published in 2004 as a result of a class on Information Security (6.805). [2] Most of the paper was concerned with non-technical details, and the short technical section claimed that MIT ID cards used amplitude-shift keying to convey information. As we found out through the course of the project, this information was either incorrect or out of date. Modern ID cards use phase-shift keying, which is significantly more sensitive to timing.

We made an effort to build a card emulator that would work with PSK:

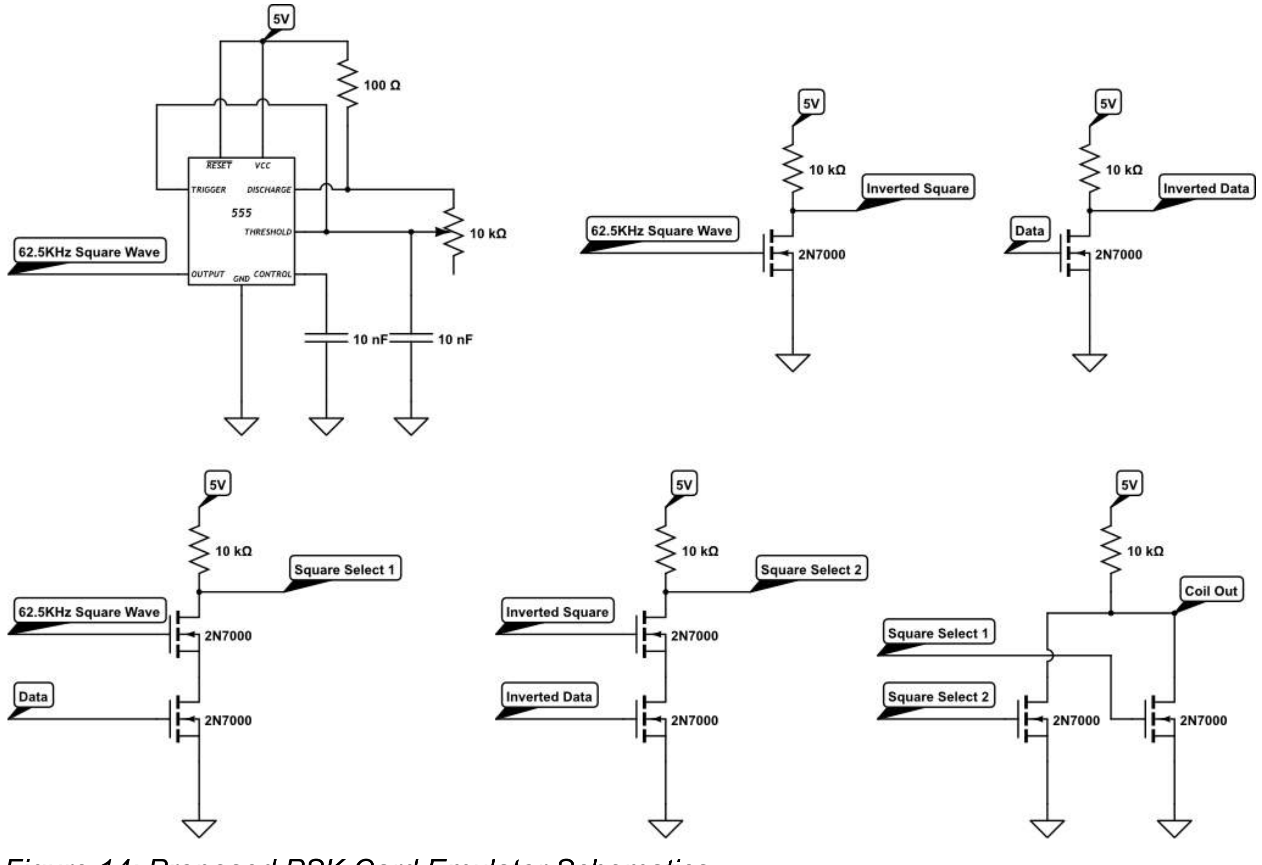


Figure 14: Proposed PSK Card Emulator Schematics

The 555 timer is used to create a square wave of 62.5KHz (half of the 125KHz carrier frequency) at approximately a 50% duty cycle. This square wave is then inverted to create one that is exactly out of phase. The "Data" node represents the same data input as the ASK card emulator. We built a multiplexer that would switch between the two square waves based on the data input. The output of the multiplexer is then fed to the ASK card emulator, which will selectively attenuate the carrier.

We were not able to get this design working. We believe this is because PSK readers are much more sensitive to timing, and the square wave output from the 555 timer was off. We likely need very close to a 50% duty cycle, and the waves should be synchronized with the carrier. A better design would somehow derive the 62.5KHz square wave by directly using the carrier, thus solving the synchronization and duty cycle issues.

Conclusion

Our project was partially successful in its goal. We were able to demonstrate that RFID could be tunneled over a distance by faking the presence of amplitude-shift keying tags. Our team learned a lot about RFID: how it works, the different methods used, and how to implement it. Given more time, we believe that we would able to accomplish our original goal of tunneling MIT RFID cards over a distance. We have already demonstrated a fundamental security flaw of RFID.

Acknowledgements

We would like to thank the following people for their support of our project:

Gim Hom (6.101 Professor) for giving us the opportunity to pursue this project.

Devon Rosner (6.101 Teaching Assistant) for his help in lab.

Mary Caulfield (Writing Advisor) for her feedback and advice regarding written materials for this project.

Works Cited

[1] Microchip, "microID® 13.56 MHz RFID System Design Guide," 2004. [Online]. Available: http://ww1.microchip.com/downloads/en/DeviceDoc/21299E.pdf. [Accessed May 19, 2014].

[2] Agrawal, Bhargava, Chandrasekhar, Dahya, Zamfirescu, "The MIT ID Card System: Analysis and Recommendations," Dec. 10, 2004. [Online]. Available: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall04-papers/mit_id/ [Accessed May 20, 2014].