Texas Academy of Math and Science
University of North Texas
College of Science
Department of Physics

Anderson Localization based Encryption

Tejas Mehta

Contents

Chapter 1

Introduction

1.1 Background Information and Motivation

In this day and age the fundamental requirement for secure communications has spread from the military industry to new industries such as hospitals, banks, and several services whose goal is to protect their user's data. Today users are starting to grow more conscious about the security of their information while using services. After major companies like Equifax and Facebook have been a victims to data breaches, thousands of users' sensitive data have been left vulnerable. The need for a novel form of encryption is at its peak.

Encryption has been an effective method in ensuring that data remains secure, however there are a few fundamental problems with several of the current technologies being used the create the problem of inefficiency, limited capability, and expensive resource use.

One of the first forms of encryption is symmetric private key encryption. The way it operates is that a user has a private key that encrypts each message and the same key is also used to decrypt the message [6]. This started with basic keys, however the algorithms have grown more and more complex to a point where the military primarily uses a form of symmetric private key encryption called the Advanced Encryption Standard or AES. The issue with AES is that it is a block cipher that encrypts each block using the same algebraic structure. [1] Although it is one of the most secure methods of encryption, it also is highly resource intensive and expensive compared to simpler forms of encryption. [7]

The alternative to private key encryption is asymmetric public key encryption. This alternative was provided because the most fundamental challenge with symmetric encryption is finding a way to securely send the key to the receiving user. The idea behind asymmetric encryption is that each user has a pair of keys, a public key and a private key. Both public and private key are linked together mathematically through a specific algorithm such that public keys are used for the encryption of data while the corresponding private key can be used for the decryption of data. [5] One of the more secure and efficient algorithms used for asymmetric encryption is Rivest–Shamir–Adleman (RSA). The issue with asymmetric encryption is that that it is quite resource intensive as well and that comes at a cost of speed as well. [6]

Both symmetric and asymmetric forms of encryption have a major issue of having keys which have the potential of being intercepted. Implementations of quantum encryption work well towards the goal of detecting whether the message or key have been intercepted through the use of principles of quantum mechanics. One example of quantum encryption is quantum key distribution. The biggest advantage of quantum key distribution is that communicating users can identify if the message being sent has been intercepted by a third party. However, if this occurs and a new key cannot be generated, the message transfer is aborted. [8]

More basic and efficient forms of encryption include frequency inversion and frequency mixing. These methods encrypt a message (usually a voice message) by inverting, adding, subtracting, or manipulating the frequencies in the message, such that the message will no longer be comprehensible. [9] The issue with this form of encryption is that the message is limited to a certain band of frequency.

The underlying issue with all of the current forms of encryption is that they are of the data encrypted have to potential to be intercepted and hacked. [8] Although it is very difficult to decrypt the data, it is possible to obtain the cipher-text of the message. Ideally the message should be impossible to even intercept or at least it should not be possible to be detected.

1.2 Goals and Theory

Encryption is typically made more secure by making the key generating algorithm more robust, however, a complex algorithm is usually resource intensive and expensive. The need for a complex key would not be present if the message would not be intercepted in the first place. The primary goal of

this research was to create a novel form of encryption in which a message can be reduced to the noise level and restored only by the intended recipient.

The quantum tunnelling phenomenon is essential towards achieving this goal. The quantum mechanics premise that particles have multiple states suggests that any particle has a different statistical probability of being in any location. This premise is what supports the phenomenon of quantum tunnelling which suggests that a particle can cross a barrier it may have not been able to cross based on Newtonian mechanics. Quantum tunneling can be seen in the nuclear fusion occurring in the sun as well the enzymes in the human body. [4]

Anderson Localization is the principle which explains the occurrence of quantum tunneling during the experiment. Anderson Localization occurs in a disordered medium in which waves do not diffuse. The random potentials in the system allow the the wave to tunnel across barriers that it could not have crossed based on the amount of kinetic energy the wave had. [3]

Both concepts apply to the encryption of messages. The medium is set up with a level of disorder. As the message crosses the medium, it is scattered infinitely, crossing numerous ”mini” barriers until the particles are homogeneous with the surrounding environment, effectively making them undetectable. [2]

Inductor Capacitor (LC) circuits were used in order to take advantage of the properties of Anderson Localization. The LC circuits mimicked the random potentials in the Anderson Localization model by utilizing varying values of capacitance and effectively creating a disordered medium for the waves to cross. [2] The LC circuits are resonant circuits in which there is a resonance frequency for each inductor and capacitor pair. The resonance frequency is dependent on the inductance and capacitance.

Chapter 2

Materials, Methods, and Procedures

2.1 Materials

The physical materials used throughout this experiment were a desktop and a laptop. The software that were used on these computers were Simulink, Matlab, and Ideal Circuit. Ideal Circuit was used to conduct AC frequency analysis. Matlab was used to create scripts that could be run on Simulink to automate the assignment of values for the inductors and capacitors. Simulink was used to conduct a transient analysis of the AC source.

2.2 Method #1

For the first method, high pass filters were combined with low pass filters to create a series of notch filters with unique resonance frequencies. Each notch in the filter effectively created a significant decay of approximately 45 db at its resonance frequency based upon the frequency analysis done in ideal circuit. The initial frequencies that were encrypted were from 28,000-48,000 hz. The resonance frequency was calculated using the resonance equation:

$$F = \frac{1}{2 * \sqrt{(L * C)}}$$

Each notch is comprised of an inductor, capacitor, and resistor as shown below in Figure 2.1:

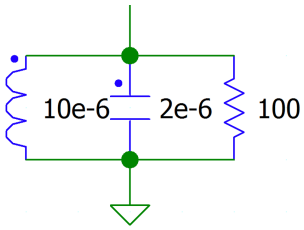

Figure 2.1: One notch

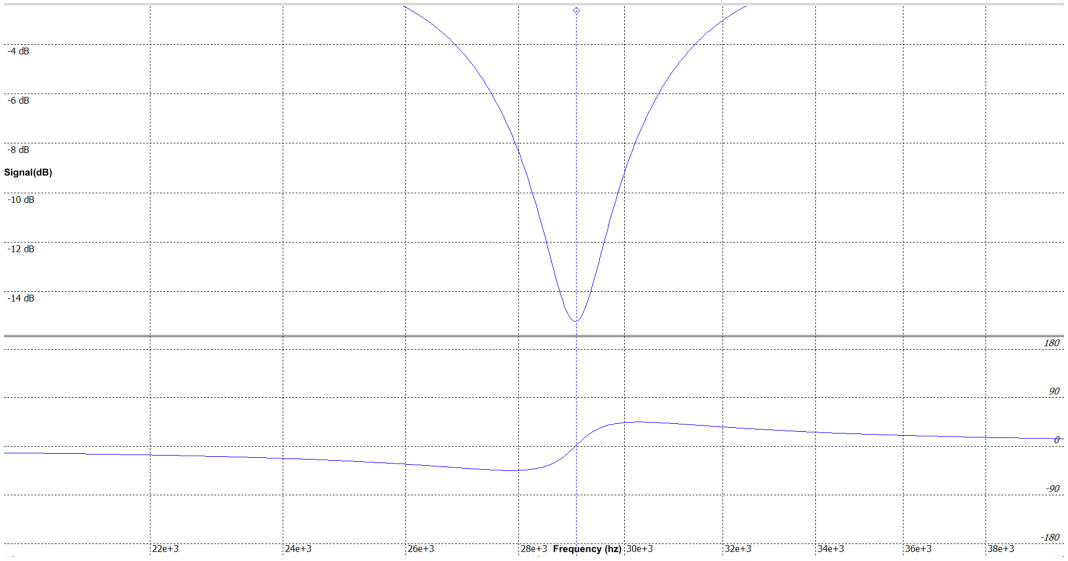

Figure 2.2: The Resonance Frequency of One Notch

The goal was for each notch's resonant frequency to be slightly offset to the previous notch so that the waves utilize destructive interference and effectively decay the signal further while widening the bandwidth of the overall "encrypted signal". Each notch's bandwidth was dependent upon the inductor value in which the lower the inductance, the bigger the bandwidth. The perfect optimization between maintaining small as possible singular notch bandwidths, effectively increasing the Q value of the circuit and minimizing error, while using around 20 components to minimize error from using too many components which all contain a small margin of error. The values of the capacitance for the capacitors were varied with each notch, representing the variation in the potentials while the inductance values of the indicators were kept constant along with the paired resistors. The first notch had an inductance of 10e-6 henrys, resistance of 100 ohms, and capacitance of 3e-6 farads. The resonance frequency for that one notch was calculated to be 29,000 hz. The result is shown in Figure 2.2: After creating a proof of concept, the targeted frequency was adjusted to a more useful frequency band such as the beginning of the AM frequency band. The targeted frequencies to encrypt were 500,000 hz to 750,000 hz. In order for this to be done 6 notches were created with an inductance of 1e-6 henrys,

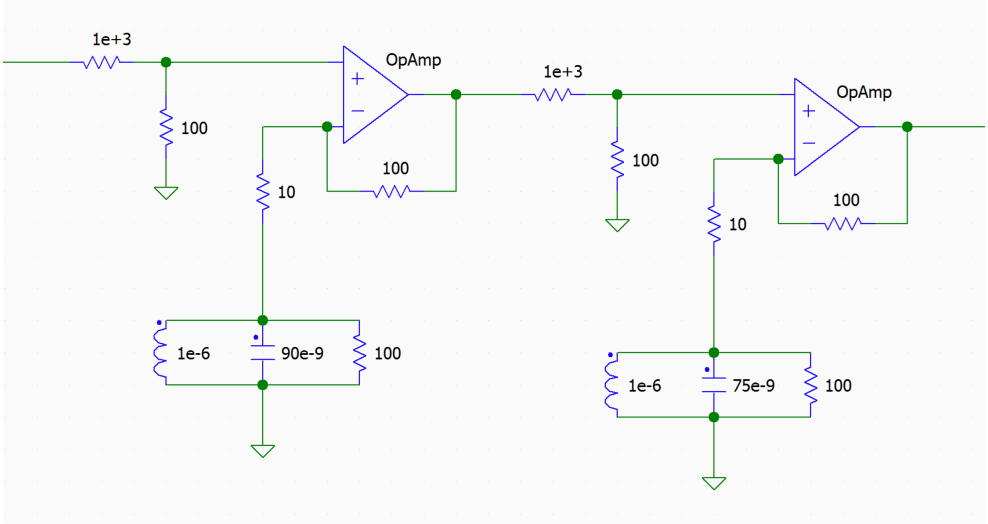

Figure 2.3: Two Notches in Series

resistance of 100 ohms, and capacitance varying from 4e-8 farads to 1.1e-7 farads. These notches were connected in series as shown in figure 2.3. For the decryption portion, the inverse of the first half of the circuit was created for each notch as shown in figure 2.4. Both portions were connected and a voltmeter was attached to the last component in each and subsequently connected to ground in order to measure the frequency. The added benefit to sticking to around 12 of each component is lower costs. Each high quality conductor with 1% tolerance costs $0.33 and each high quality inductor with 1% tolerance is $1.85. Adding the cost of each operational amplifier to be $2.81 per component led to a total cost of the encryption and decryption filter being simply $59.88.

After determining the ideal situation to be a success, the situation had to be tested with having remnant noise. In order for this to be tested, the circuit was transferred to Simulink using Simscape components. To simulate the noise that would still exist, a voltage source with a slightly higher maximum amplitude than the decayed signal and a random period was input after the encryption portion of the circuit. Data was then measured to see the effect of noise on the experiment.

2.3 Method #2

Since the circuit in Method 1 did not work after noise was added, an alternative circuit design was devised. In this approach, a large number of LC circuits were connected in parallel with randomized capacitor values. The greater the variance in the capacitance, the greater the overall disorder of the

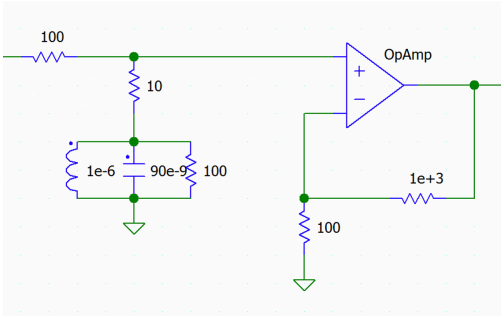

Figure 2.4: The Inverse of One Notch

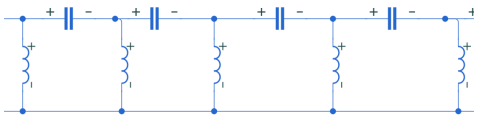

Figure 2.5: Several LC components connected in parallel

circuit. The alternative to increasing disorder in simply using more components. For this experiment, 40 inductor/capacitor pairs connected in parallel as shown in figure 2.5 with an inductance of 10e-6 henrys and capacitance randomly generated with values between 1.12e-5 farads and 3.26e-5 farads. For the decryption, a statistically correlated version of the first with the same structure was created.

Chapter 3

Data and Analysis

3.1 Method #1 Results

Looking at figure 3.1, the goal to encrypt the frequencies from 500 kHz to 750 kHz has been achieved as the signal intensity for all values in that frequency range is less than or equal to -30dB which is sufficient decay which can be seen by the blue green line. The goal to restore the signal to the original signal was mostly achieved although there was a slight error that was depicted by the blue line. The original AC signal can be seen by the red line.

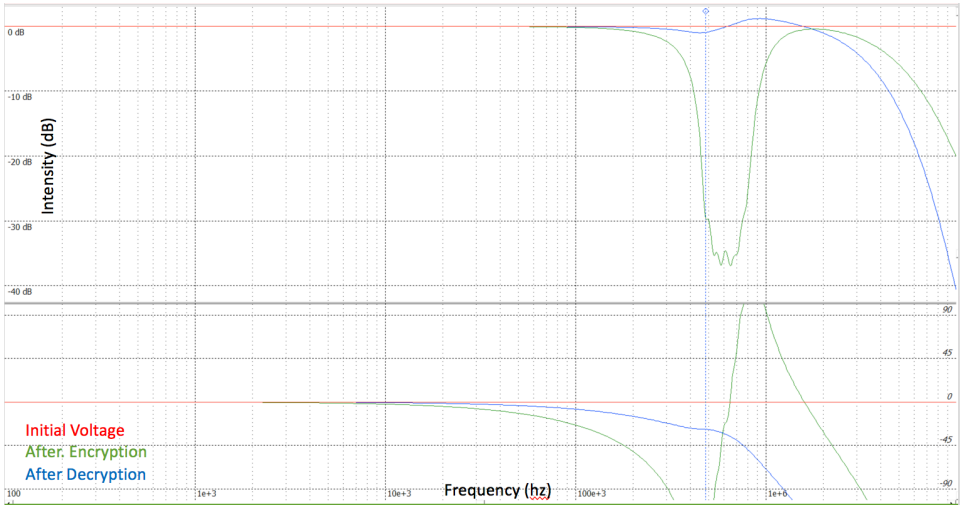

Figure 3.1: The Frequency Analysis of the full notch filter

The similar results were shown in a transient analysis of a specific frequency within the range in Figure

3.2. 96% of the signal was decayed after the encryption portion of the circuit which is enough to keep it below the noise level and describes significant decay. The yellow curve describes the signal after the encryption while the purple curve describes the original AC signal.

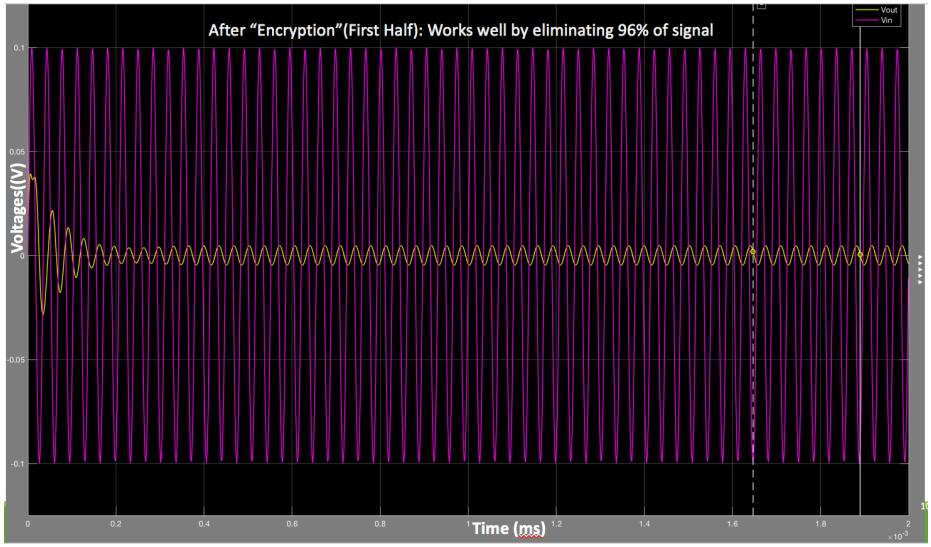

Figure 3.2: Transient Analysis of Encryption Circuit

More encouraging results were shown in Figure 3.3, in which the yellow and purple curve have overlapped each other. The yellow curve describes the signal after the decryption while the purple curve describes the original AC signal. Since both curves are at the same location and therefore the signal has been 100% restored.

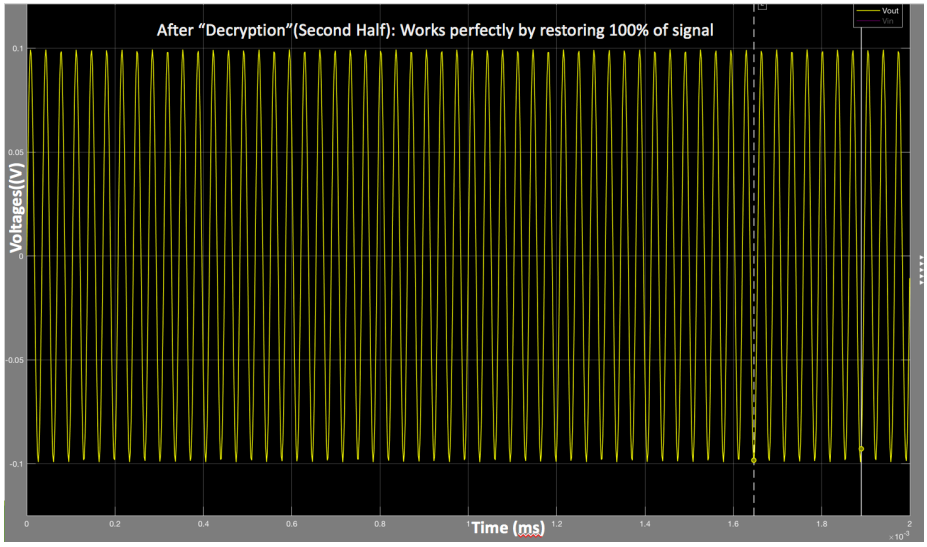

Figure 3.3: Transient Analysis of Decryption Circuit

After adding a voltage source with a maximum amplitude similar to the encrypted signal with a random period and amplitude using Matlab's random noise algorithm, results for the encryption circuit were recorded and are displayed in Figure 3.4. The majority of the graph is similar to Figure 3.2 with almost 96% loss of signal however there are several small anomalies in the graph that may have been created due the highest and lowest voltages of the noise.

Figure 3.4: Transient Analysis of Encryption Circuit with added noise

The simulated noise voltage source creates problems in Figure 3.5 which depicts the transient analysis of the the decryption circuit with added noise. The decryption successfully restored the original signal, but also amplified the noise. The decrypted signal would not be usable in this case and therefore, this test failed. This implies that this model did not display attributes of Anderson localization, as in a true Anderson Localization model, noise would be supressed.

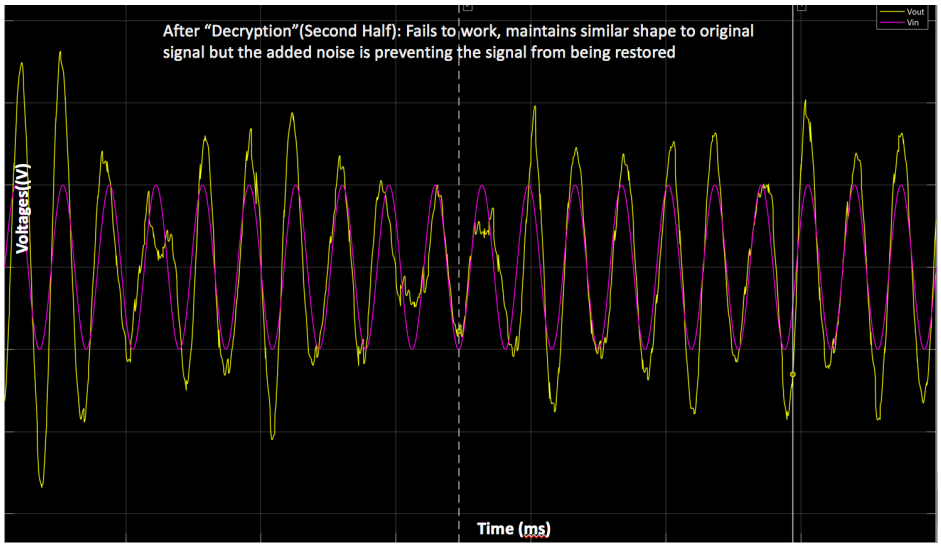

Figure 3.5: Transient Analysis of Decryption Circuit with added noise

3.2 Method #2 Results

After creating the circuit described in method #2, a transient analysis of the encryption circuit was conducted and the results are shown in Figure 3.6. The signal decay is happening periodically, which is a characteristic of true Anderson Localization. At its lowest points, the voltage amplitude almost approaches exactly zero with an error of less than 1% demonstrating very effective signal decay.

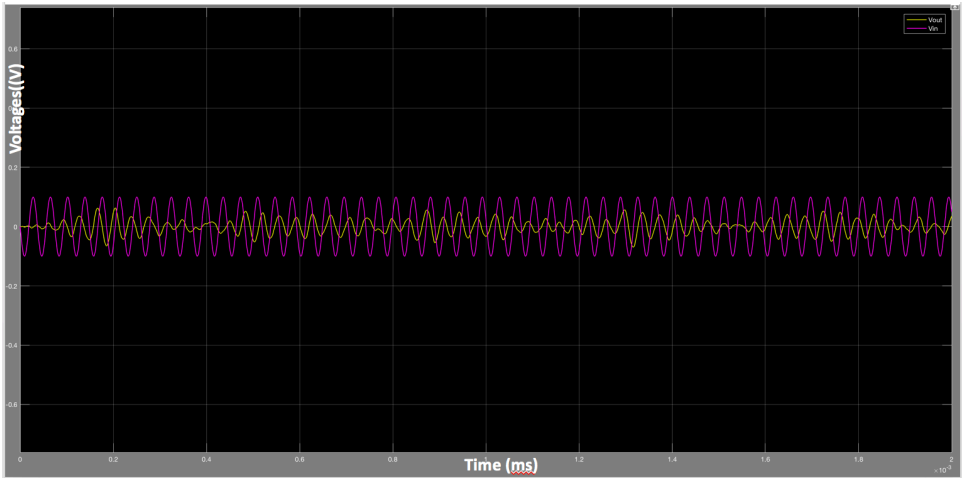

Figure 3.6: Transient Analysis of Encryption Circuit

Similar results were displayed in the transient analysis of the decryption circuit. The restoration of the

signal occurred periodically following the same pattern as the encryption circuit. The times when the signal decayed in the encryption circuit, the signal was restored in the decryption circuit. The restored signal was almost exactly the sane as the original signal with a very small error of less than 1% in some places. The error could be reduced by increasing the disorder in the system by either introducing more LC pairs into the circuit, or by increasing the variance of the capacitors.

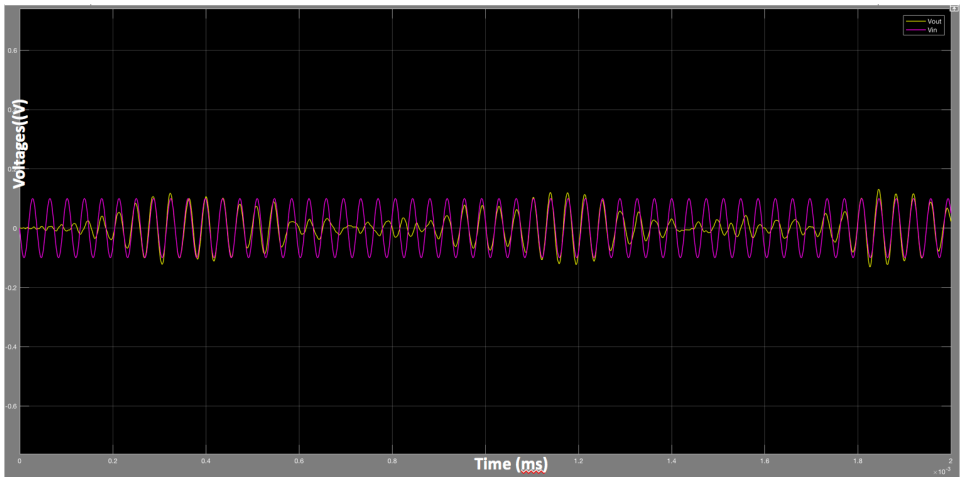

Figure 3.7: Transient Analysis of Decryption Circuit

Chapter 4

Conclusions

4.1 Analysis of Results

The goal for method #1 was to create a series of notch filters which would reduce a signal to the noise level and restore the signal with the inverse of the notch filters. Specifically the goals was to complete the objective above for 500 kHz - 750 kHz (The beginning of the AM frequency band). This goal was met in ideal conditions as according to figure 3.1, the signal significantly decayed after going through the encryption portion of the circuit and mostly restored after going through the decryption portion of the circuit. In order to test whether Anderson Localization is present, the random ”noise” voltage source was used to simulate real-life white noise. After introducing the noise, anomalies began to occur and the decryption portion restored not only the signal, but also the noise, leading to an end result which had little resemblance to the original signal. Overall the notch filter approach was a cheap, secure, and efficient approach to encryption and decryption, however, it will only work well in ideal conditions or components with very high Q values and low tolerances.

The second approach had the same goal as method #1; however, the circuit design was fundamentally different. Inductors and Capacitors were connected in parallel rather than series and resistors and Operational Amplifiers were not necessary. Based on figures 3.6 and 3.7, the original engineering goal was completed successfully. Figure 3.6 displayed more than 99% of the signal being encrypted during some times and figure 3.7 displayed a signal with an amplitude with less than a 1% difference to the amplitude of the original signal at some times. The encryption and decryption happened periodically with a 0 degree phase shift which gives strong evidence that the model is undergoing quantum tunnel-

ing and Anderson Localization. The error could be reduced by increasing the disorder in the system by either introducing more LC pairs into the circuit, or by increasing the variance of the capacitors. Both methods achieved the engineering goal to some extent, although approach #2 was much more versatile and displayed true Anderson Localization.

4.2 Applications and Future Work

Work is currently being done in increasing the disorder of the system built in approach #2. In order to this a circuit of 140 LC pairs is under construction with capacitors with a higher variance. Also errors need to be introduced to the components in the simulation, to ensure that the results can be replicated. After that prototypes for the actual filters will be developed.
Currently, the most obvious application for this technology, is secure military communications. Echonovus Inc is currently pursuing a Small Business and Innovative Research (SBIR) grant to utilize this encryption technology for fighter jet intra-cockpit secure wireless communications. Hospitals could also take advantage of this technology to safely transmit sensitive medical records. In the future, there are plans to utilize this technology with digital technology. This will allow secure communications in any industry and the technology can even benefit the common man. Business networks, banking networks, and high sensitivity government networks such as the National Security Agency can all benefit from this technology.

4.3 Current Work: Automation of Circuit

Currently most work is being devoted towards building a significantly larger circuit with high disorder. As the size of the circuit is quite high building the circuit manually yielded ineffectual as the computer's processor was not able to handle the number of the components and the Graphical User Interface at the same time. In order to streamline the process for circuit-building, the solution was create programmatically. Using MATLAB to program the circuit worked to successfully model the circuit of high disorder which should theoretically display higher levels of localization and antilocalization in both the ”encryption” and the ”decryption” respectively. Testing is currently being conducted, although the algorithm needs to be modified to be more efficient as the run time to create a circuit of

500 components was approximately 30 minutes simply to build the circuit. The algorithm to set the values of the components and built the circuit can be found below and is fully complete.

4.4 Appendix for Code

```
cappos = [60 72 90 88];
indpos = [92 90 108 120];
total = 500;
bigTotal = total*2;
add_block('fl_lib/Electrical/Electrical Elements/Capacitor',[sys sprintf('/Cap%d',
    1)], 'Position', cappos);
    cappos(1) = cappos(1)+60;
    cappos(3) = cappos(3)+60;
    add_block('fl_lib/Electrical/Electrical Elements/Inductor',[sys
        sprintf('/Ind%d', 1)], 'Position', indpos, 'Orientation', 'down');
    indpos(1) = indpos(1)+60;
    indpos(3) = indpos(3)+60;
    add_line(sys, sprintf('Cap%d/RConn1', 1), sprintf('Ind%d/LConn1',
        1)','autorouting','on')


for i = 2:total\\
    add_block('fl_lib/Electrical/Electrical\\ Elements/Capacitor',[sys
        sprintf('/Cap%d', i)], 'Position', cappos);
    add_line(sys, sprintf('Cap%d/RConn1', i-1), sprintf('Cap%d/LConn1',
        i)','autorouting','on')
    cappos(1) = cappos(1)+60;
    cappos(3) = cappos(3)+60;
    add_block('fl_lib/Electrical/Electrical Elements/Inductor',[sys
        sprintf('/Ind%d', i)], 'Position', indpos, 'Orientation', 'down');
    indpos(1) = indpos(1)+60;
    indpos(3) = indpos(3)+60;
```

```
    add_line(sys, sprintf('Ind%d/RConn1', i-1), sprintf('Ind%d/RConn1',
        i)','autorouting','on')
    add_line(sys, sprintf('Cap%d/RConn1', i), sprintf('Ind%d/LConn1',
        i)','autorouting','on')
end\\

add_block('fl_lib/Electrical/Electrical Elements/Inductor',[sys sprintf('/Ind%d',
    bigTotal+1)], 'Position', indpos, 'Orientation', 'down');
add_line(sys, sprintf('Ind%d/RConn1', total), sprintf('Ind%d/RConn1',
    bigTotal+1)','autorouting','on')
add_line(sys, sprintf('Ind%d/LConn1', total), sprintf('Ind%d/LConn1',
    bigTotal+1)','autorouting','on')

 cappos(1) = cappos(1)+60;
 cappos(3) = cappos(3)+60;
 indpos(1) = indpos(1)+60;
 indpos(3) = indpos(3)+60;

 add_block('fl_lib/Electrical/Electrical Elements/Capacitor',[sys sprintf('/Cap%d',
     total+1)], 'Position', cappos);
    add_line(sys, sprintf('Ind%d/LConn1', bigTotal+1), sprintf('Cap%d/LConn1',
        total+1)','autorouting','on')
    cappos(1) = cappos(1)+60;
    cappos(3) = cappos(3)+60;
    add_block('fl_lib/Electrical/Electrical Elements/Inductor',[sys
        sprintf('/Ind%d', total+1)], 'Position', indpos, 'Orientation', 'down');
    indpos(1) = indpos(1)+60;
    indpos(3) = indpos(3)+60;
    add_line(sys, sprintf('Ind%d/RConn1', bigTotal+1), sprintf('Ind%d/RConn1',
        total+1)','autorouting','on')
    add_line(sys, sprintf('Cap%d/RConn1', total+1), sprintf('Ind%d/LConn1',
        total+1)','autorouting','on')

for i = total+2:bigTotal\\
```

```
    add_block('fl_lib/Electrical/Electrical Elements/Capacitor',[sys
        sprintf('/Cap%d', i)], 'Position', cappos);
    add_line(sys, sprintf('Cap%d/RConn1', i-1), sprintf('Cap%d/LConn1',
        i)','autorouting','on')
    cappos(1) = cappos(1)+60;
    cappos(3) = cappos(3)+60;
    add_block('fl_lib/Electrical/Electrical Elements/Inductor',[sys
        sprintf('/Ind%d', i)], 'Position', indpos, 'Orientation', 'down');
    indpos(1) = indpos(1)+60;
    indpos(3) = indpos(3)+60;
    add_line(sys, sprintf('Ind%d/RConn1', i-1), sprintf('Ind%d/RConn1',
        i)','autorouting','on')
    add_line(sys, sprintf('Cap%d/RConn1', i), sprintf('Ind%d/LConn1',
        i)','autorouting','on')
end

add_line(sys, sprintf('Cap%d/LConn1', 1), sprintf('Ind%d/RConn1',
    1)','autorouting','on')
add_block('fl_lib/Electrical/Electrical Elements/Electrical Reference',[sys
    '/Ground'], 'Position', [30 170 50 190]);
add_line(sys, 'Ground/LConn1', sprintf('Ind%d/RConn1', 1)','autorouting','on')


%get_param('vdp','ObjectParameters')

v = 0;
r = 0;
m = "";
s = "";
num = 0;
r = (1.12e-5) + ((3.26e-5) - (1.12e-5)).*rand(250,1)
for v = 1:1:80
    template = 'testModel/Capacitor';
```

```
    m = int2str(v);
    num = sprintf('%.8f',r(v));
    s = strcat(template,m);
    set_param(s,'c',num);
    m = int2str(501-v);
    s = strcat(template,m);
    set_param(s,'c',num);
end
for p = 1:1:500
    template = 'testModel/Inductor';
    m = int2str(p);
    s = strcat(template,m);
    set_param(s,'l','1e-6');
    set_param(s,'g','0');
end
```

Bibliography

[1] "Advantages of AES | disadvantages of AES," *RF Wireless World*. [Online]. Available: http://www.rfwireless-world.com/Terminology/Advantages-and-disadvantages-of-AES.html. [Accessed: 11-Oct-2018].

[2] E. Diez, F. Izrailev, A. Krokhin, and A. Rodriguez, "Symmetry-induced tunneling in one-dimensional disordered potentials," *Physical Review B*, vol. 78, no. 3, 2008.

[3] A. Lagendijk, B. V. Tiggelen, and D. Wiersma, "Notes on Anderson localization," *Physics Today*, vol. 65, no. 5, pp. 11–12, Aug. 2009.

[4] L. Mastin, "Quantum Tunneling and the Uncertainty Principle," *Quantum Tunneling and the Uncertainty Principle - Quantum Theory and the Uncertainty Principle - The Physics of the Universe*. [Online]. Available: https://www.physicsoftheuniverse.com/topics_quantum_uncertainty.html.

[5] M. Rouse, "What is asymmetric cryptography (public key cryptography)?," *SearchSecurity*, Jun-2016. [Online]. Available: https://searchsecurity.techtarget.com/definition/asymmetric-cryptography. [Accessed: 11-Oct-2018].

[6] "Symmetric vs. Asymmetric Encryption – What are differences?," *SSL2BUY Wiki - Get Solution for SSL Certificate Queries*, 07-Oct-2017. [Online]. Available: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences. [Accessed: 11-Oct-2018].

[7] "What is AES encryption?," *IT PRO*, 10-May-1970. [Online]. Available: http://www.itpro.co.uk/security/29671/what-is-aes-encryption. [Accessed: 11-Oct-2018].

[8] B. D. Hayford, "The Future of Security: Zeroing In On Un-Hackable Data With Quantum Key Distribution," Wired, 07-Aug-2015. [Online]. Available: https://www.wired.com/insights/2014/09/quantum-key-distribution/. [Accessed: 11-Oct-2018].

[9] E. Jacobsen, "Handling Spectral Inversion in Baseband Processing," DSPRelated.com | DSP. [Online]. Available: https://www.dsprelated.com/showarticle/51.php. [Accessed: 11-Oct-2018].