5-2017

A Practical Realization of a Return Map Immune Lorenz Based Chaotic Stream Cipher in Circuitry

Daniel Robert Brown
University of Tennessee, Knoxville, dbrown63@vols.utk.edu

Recommended Citation

Brown, Daniel Robert, "A Practical Realization of a Return Map Immune Lorenz Based Chaotic Stream Cipher in Circuitry. " Master's Thesis, University of Tennessee, 2017.
https://trace.tennessee.edu/utk_gradthes/4727

To the Graduate Council:

I am submitting herewith a thesis written by Daniel Robert Brown entitled "A Practical Realization of a Return Map Immune Lorenz Based Chaotic Stream Cipher in Circuitry." I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Electrical Engineering.

Donatello Materassi, Major Professor

We have read this thesis and recommend its acceptance:

Seddik Djouadi, Nicole McFarlane, Max Schuchard

Accepted for the Council:
Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

A Practical Realization of a Return Map Immune Lorenz Based Chaotic Stream Cipher in Circuitry

A Thesis Presented for the

Master of Science

Degree

The University of Tennessee, Knoxville

Daniel Robert Brown

May 2017

For my son, Gordon.

Chaos: When the present determines the future, but the approximate present does not approximately determine the future.

Abstract

Some chaotic systems are advantageously capable of self-synchronizing with a like system through a single shared state. Using a plain text binary message, a single system parameter can be modulated to mask this message and transmit it securely through the single shared state. The most simple implementations of this encryption technique are, however, vulnerable to the return map attack. Using a time-scaling factor to further obfuscate the modulation process, a return map attack immunity is gained. We report on the progress towards a realization of this process in real-time analog circuitry using off-the-shelf components.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

On a cold winters day in January 1917 the value of strong encryption and the damage weak security can cause were made known. British intelligence in Room 40 intercepted a diplomatic cable from Germany to Mexico. This coded message was broken, and the realization of German intentions to make Mexico its ally against the United States (Pincock, 2006, CH. 4). This news, once public, along with Germany's continuation of unrestricted submarine warfare on passenger and merchant ships lead the United States into the Great War. The Germans would fall prey to a broken cipher again in the Second World War with the failure of the far more complex Enigma (Sebag-Montefiore, 2011).

Cryptography and the use of ciphers can be traced to much earlier in human history. Cryptanalysis methods and code breaking can be traced back to the work of Al-Kindi, who developed a frequency-analysis method for breaking substitution ciphers (Pincock, 2006, CH. 1). Privacy and secrecy has only become more necessary and complex as history has continued to present day. The importance is easy to see from examples of military history, but even encryption for private citizens is now necessary with the common place use of online banking and shopping.

The digital computer has allowed the usage of cheap, fast and automatic encryption to become possible. However the computer, even in rudimentary forms such as the

Bombe machines that broke the Enigma (Keen, 2003), has improved code cracking capabilities. At a minimum the computer has exponentially increased the speed at which brute force methods can function. To combat this capability, methods such as asymmetric ciphers (Rivest et al., 1978) and symmetric ciphers (Daemen and Rijmen, 2013) have been designed to take advantage of computational capabilities of modern machines. These methods however require computational overhead and offer with each use only one layer of encryption.

Chaotic encryption seeks to provide a second method of security through masking of data with a chaotic system that is highly sensitive to system parameters and initial conditions (Lu et al., 2002). This usage of a non-linear system allows for a layered encryption over a bit-wise encrypted signal. Methods exist to use maps (Makris and Antoniou, 2012) as well as using chaotic non-linear system models (Liu and Tsimring, 2006). This work studies the use of the latter, the use of a non-linear system model to mask a binary plain text message known as Chaotic Shift Keying (CSK). We seek to use a minimal amount of processing power to accomplish such a goal. We plan to provide a method of encryption to low processing power applications, as well as provide a second layer of encryption to already encrypted digital data.

1.1 Organization

This thesis is organized into chapters to cover the practicality of a Lorenz based chaotic stream cipher. Chapter 2 will provide necessary background on the use of a chaotic stream cipher, the vulnerabilities of such a system, and the time-scaling factor added to increase security. Chapter 2 will also give a brief basic background of the circuitry fundamentals. Chapter 3 covers the practical implementation of the CSK system, in simulation and in circuitry. Chapter 3 will also cover the methods and metrics of the system performance analysis. Chapter 4 contains the results of the simulated and practical systems. Chapter 5 is the discussion of the results and conclusion of this work.

Chapter 2

Background

2.1 The Lorenz Chaotic System

In 1963, Edward Lorenz created model for simulating convectional flow in the atmosphere (Lorenz, 1963). This model showed, for certain parameter ranges, interesting tendencies of which small changes in initial conditions lead to significantly different outcomes later within the system. This system as described by Lorenz (1963) is shown below:

$$\begin{aligned} \dot{x} &= \sigma(y - x) \\ \dot{y} &= (\beta - z)x - y \\ \dot{z} &= xy - \rho z \end{aligned} \tag{2.1}$$

The parameters β,ρ, and σ are real positive values, and only certain value ranges and relations result in a chaotic system. In relation to Lorenz's original use for this system, β and σ are the Rayleigh number and Prandtl number. ρ is based on the physical proportion (Sparrow, 2012).

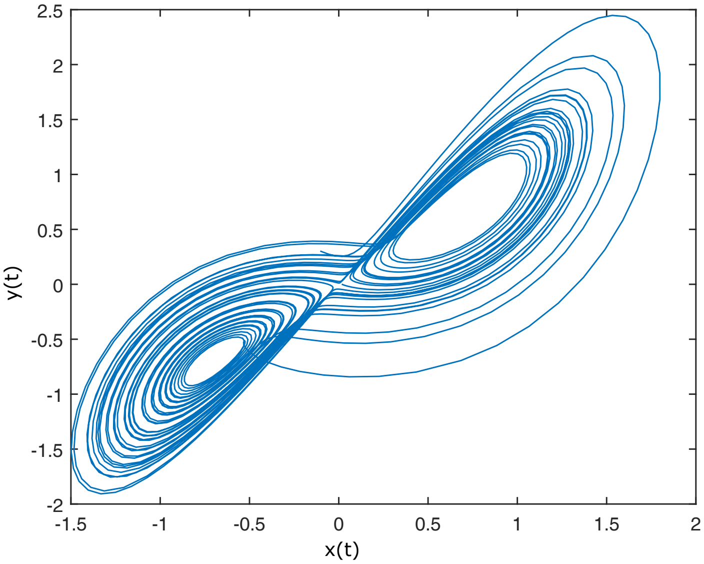


Figure 2.1: A plot of x vs y from the Lorenz system, this is commonly referred to as the butterfly attractor

2.1.1 System Characteristics

To show that certain parameter choices lead to asymptotic stability, rather than the chaotic behavior as seen in Figure 2.1, one can use a Lyapunov function.

$$\begin{aligned} V(x,y,z,t) &= \frac{1}{2\sigma}x^2 + \frac{1}{2}y^2 + \frac{1}{2}z^2 && (2.2) \\ \dot{V}(x,y,z,t) &= \frac{1}{\sigma}\dot{x} + y\dot{y} + z\dot{z} \\ &= -x^2 + xy + \beta xy - xyz - y^2 + xyz - \rho z^2 \\ &= -x^2 + (1+\beta)xy - y^2 - \rho z^2 \\ &= -\Big(\frac{1+\beta}{2}x - y\Big)^2 + \Big(\frac{(1+\beta)^2}{4} - 1\Big)x^2 - \rho z^2 && (2.3) \end{aligned}$$

The Lyapunov equation (2.2) is positive definite and $V(x, y, z, t) = 0$ iff $x, y, z = 0$. The time derivative, $\dot{V}(x, y, z, t)$, is also negative definite for all selections of $\beta \leq 1$.

$$\begin{aligned} \frac{(1+\beta)^2}{4} - 1 &< 0 \\ \beta^2 + 2\beta - 3 &< 0 \\ (\beta - 1)(\beta + 3) &< 0 \end{aligned} \tag{2.4}$$

This can be viewed in the terms of equilibrium of the system as well. The Lorenz system has equilibrium:

$$\begin{aligned} 0 &= y - x \\ 0 &= (\beta - z)x - y \\ 0 &= xy - \rho z \end{aligned}$$

This will lead to the relationships of:

$$\begin{aligned} x &= y \\ z &= \beta - 1 \\ x &= \pm\sqrt{\rho(\beta - 1)} \end{aligned}$$

As such the equilibrium of the Lorenz system are:

$$\alpha = \begin{Bmatrix} (0, 0, 0) \\ \Big(\sqrt{\rho(\beta-1)}, \sqrt{\rho(\beta-1)}, \beta - 1\Big) \\ \Big(-\sqrt{\rho(\beta-1)}, -\sqrt{\rho(\beta-1)}, \beta - 1\Big) \end{Bmatrix} \tag{2.5}$$

Clearly when $\beta \leq 1$ the only existing real equilibrium is (0,0,0). The nature of the origin in context to the system as a whole is shown below with the Jacobian matrix.

$$J_{\alpha_0} = \begin{bmatrix} -\sigma & \sigma & 0 \\ \beta & -1 & 0 \\ 0 & 0 & -\rho \end{bmatrix} \tag{2.6}$$

The eigenvalues of J_{α_0} are then found as:

$$\lambda_J = \left\{ \begin{matrix} -\frac{1}{2}\left(\sigma + 1 - \sqrt{\sigma^2 + (4\beta - 2)\sigma + 1}\right) \\ -\frac{1}{2}\left(\sigma + 1 + \sqrt{\sigma^2 + (4\beta - 2)\sigma + 1}\right) \\ -\rho \end{matrix} \right\} \tag{2.7}$$

The last two possible eigenvalues, λ_{J2} and λ_{J3} will always have a real part < 0. However the first eigenvalue, λ_{J1} will have real part > 0 when:

$$\begin{aligned} \sigma + 1 &< \sqrt{\sigma^2 + (4\beta - 2)\sigma + 1} \\ \sigma^2 + 2\sigma + 1 &< \sigma^2 + (4\beta - 2)\sigma + 1 \\ 2 &< 4\beta - 2 \\ \beta &> 1 \end{aligned}$$

This result indicates that as β becomes greater than 1, the origin becomes unstable and two more equilibrium appear. Another interesting relationship of the Lorenz system can be extracted from the eigenvalues (λ_J) of the Jacobian about the origin. Sparrow cites a unique relationship about these eigenvalues that is:

$$-\lambda_{J3} < \lambda_{J1} < -\lambda_{J2} \tag{2.8}$$

Under the condition that:

$$\beta > 1 + \frac{\rho(\sigma + 1 + \rho)}{\sigma} \tag{2.9}$$

To gather further behavioral characteristics of the Lorenz system, the Jacobian matrices for the two other equilibrium are calculated.

$$J_{\alpha_1} = \begin{bmatrix} -\sigma & \sigma & 0 \\ 1 & -1 & -\sqrt{\rho(\beta-1)} \\ \sqrt{\rho(\beta-1)} & \sqrt{\rho(\beta-1)} & -\rho \end{bmatrix} \tag{2.10}$$

The characteristic equation of the Jacobian, $|\lambda I - J_{\alpha_1}| = 0$, is then found as:

$$\lambda^3 + (\sigma + \rho + 1)\lambda^2 + \rho(\sigma + \beta)\lambda + 2\sigma\rho(\beta - 1) = 0 \tag{2.11}$$

Calculating the roots generically is cumbersome and not necessary for evaluation of the Lorenz system in respect to chaotic encryption. There is an alternate method at which to approach the roots of the equilibrium α_1 and α_2 such as to guarantee chaotic behavior. The roots that are desired are those that create a Hopf bifurcation (Sparrow, 2012). These can be found by selecting a σ and ρ such that the discriminate of (2.11) is negative $\forall\ \beta > 1$.

$$\Delta = 18w_0w_1w_2 - 4w_2^3w_0 + w_2^2w_1^2 - 4w_1^3 - 27w_0^2 \tag{2.12}$$

Where:

$$w_0 = 2\sigma\rho(\beta - 1)$$
$$w_1 = \rho(\sigma + \beta)$$
$$w_2 = \sigma + \rho + 1$$

In the case that $\Delta < 0$ the eigenvalues consist of one real value and two complex values (Irving, 2003). This is a useful property for making relations of (2.11) to chaotic behavior. Specifically it is desired that α_1 and α_2 be linearly unstable (Sparrow, 2012). This transition will occur at $\lambda = \pm qi$, where $i = \sqrt{-1}$ and q is real and positive. Setting $\lambda = qi$ in (2.11) yields:

$$\begin{aligned} -q^3 i - (\sigma + \rho + 1)q^2 + \rho(\sigma + \beta)qi + 2\sigma\rho(\beta - 1) &= 0 + 0i \\ (-(\sigma + \rho + 1)q^2 + 2\sigma\rho(\beta - 1)) + q(-q^2 + \rho(\sigma + \beta))i &= 0 + 0i \end{aligned}$$

As such

$$\begin{aligned} -q^2 + \rho(\sigma + \beta) &= 0 \\ \rho(\sigma + \beta) &= q^2 \end{aligned} \qquad \begin{aligned} -(\sigma + \rho + 1)q^2 + 2\sigma\rho(\beta - 1) &= 0 \\ 2\sigma\rho(\beta - 1) &= -(\sigma + \rho + 1)q^2 \\ \frac{2\sigma\rho(\beta - 1)}{\sigma + \rho + 1} &= q^2 \end{aligned}$$

Merging the two equations together to find the Hopf bifurcation point β_h

$$\begin{aligned} \rho(\sigma + \beta_h) &= \frac{2\sigma\rho(\beta_h - 1)}{\sigma + \rho + 1} \\ \rho(\sigma - \rho - 1)\beta_h &= \rho\sigma(\sigma + \rho + 3) \\ \beta_h &= \frac{\sigma(\sigma + \rho + 3)}{\sigma - \rho - 1} \end{aligned} \tag{2.13}$$

As can be seen by (2.13) for $\beta_h > 0$ the conditions of σ and ρ can be constrained such that:

$$\sigma > \rho + 1 \tag{2.14}$$

The necessary constraints for chaotic behavior are then determined by (2.13) and (2.14).

2.1.2 Boundedness Condition

The Lorenz equation is bounded for all positive real parameter selections. It is obvious from the results of (2.7) that for $\beta \leq 1$ the system is stable and therefore bounded. To show that the solutions of (2.1) are bounded for $\beta > 1$, Swinnerton-Dyer suggests a Lyapunov function:

$$\begin{aligned} V &= a_1x^2 + a_2(y^2 + z^2) + 2a_3z && (2.15) \\ \dot{V} &= 2a_1x\dot{x} + 2a_2(y\dot{y} + z\dot{z}) + 2a_3\dot{z} \\ &= -2a_1\sigma x^2 - 2a_2y^2 - 2a_2\rho z^2 + (2a_1\sigma + 2a_2\rho + 2a_3)xy - 2a_3\rho z && (2.16) \end{aligned}$$

Rather than using the Lyapunov function relations described by Slotine et al. and used in other Lyapunov function examples in this thesis, Swinnerton-Dyer suggests the relation:

$$\dot{V} + \lambda(V - c) \leq 0 \tag{2.17}$$

This more general application of Lyapunov stability theory allows one to state that $V > c \implies \dot{V} < 0$. As such, if a function V can be found such that (2.17) is true, then the system described by V is bounded by at least $V = c$. As such:

$$a_1(\lambda - 2\sigma)x^2 + a_2(\lambda - 2)y^2 + a_2(\lambda - 2\rho)z^2 + 2(a_1\sigma + a_2\beta + a_3)xy + 2a_3(\lambda - \rho)z - \lambda c < 0 \tag{2.18}$$

From (2.18) Swinnerton-Dyer details required constraints such that (2.17) is true.

$$\begin{aligned} a_1(\lambda - 2\sigma) &\leq 0 & a_2(\lambda - 2\rho) &\leq 0 \\ a_2(\lambda - 2) &\leq 0 & c &\geq 0 \\ (\sigma a_1 + \beta a_2 + a_3)^2 &\leq a_1a_2(2\sigma - \lambda)(2 - \lambda) & \lambda c a_2(2\rho - \lambda) &\geq a_3^2(\rho - \lambda)^2 \end{aligned} \tag{2.19}$$

A set Ω_V is then described as the set such that $V \leq c$ and is the bounded region of operation for (2.1). To determine Ω_V and hold (2.19) true, Swinnerton-Dyer sets:

$$\begin{aligned}
c &= \frac{a_3^2(\rho-\lambda)^2}{a_2\lambda(2\rho-\lambda)} \\
a_3 &= -\sigma a_1 - \beta a_2 \\
a_1 &> 0 \\
a_2 &> 0 \\
0 < \lambda &< \min(2, 2\rho)
\end{aligned}$$

The bounding condition and set Ω_V is then described as:

$$a_1x^2 + a_2y^2 + a_2\Big(z - \frac{a_1\sigma + a_2\beta}{a_2}\Big)^2 \leq \frac{\rho^2(a_1\sigma + a_2\beta)^2}{\lambda a_2(2\rho-\lambda)} \tag{2.20}$$

2.2 Chaotic Synchronization

Two like chaotic systems with different starting initial conditions can be matched to the same trajectory by coupling the two systems with a single state shared from one to the other. This process is known as chaotic synchronization (Pecora and Carroll, 1990). The system providing the shared state is known as the drive system, conversely the second system is the driven system. Pecora and Carroll show experimentally that the Lorenz system also has a strict tolerance of system parameter matching for synchronization to occur.

This property of synchronization in chaotic systems can be exploited to generate an encryption mask. Oppenheim et al. demonstrate the use of a Lorenz chaotic system for analog speech signal encryption. An analog speech signal however limits the type of information that be transmitted securely. Cuomo and Oppenheim and Dedieu et al. demonstrate the masking of a binary signal with chaos with a Lorenz system and Chua's circuit respectively. This method of masking a binary system, known as chaotic shift keying (CSK), has wider use in communication systems of the modern world. CSK accommodates the capabilities of a digital signal, such as checksum error detection and bit wise encryption methods.

$$\begin{aligned} \dot{x}_1 &= \sigma(x_2 - x_1) & \dot{z}_1 &= \sigma(z_2 - z_1) \\ \dot{x}_2 &= (\beta(m) - x_3)x_1 - x_2 & \dot{z}_2 &= (\beta_0 - z_3)x_1 - z_2 \\ \dot{x}_3 &= x_1x_2 - \rho x_3 & \dot{z}_3 &= x_1z_2 - \rho z_3 \end{aligned} \tag{2.21}$$

Equation set (2.21) describes a Lorenz based CSK system. The forcing system, or transmitter, being represented by x_1, x_2, x_3 and the forced system, or receiver, represented by z_1, z_2, z_3. The parameter β is used as a binary variable gain to mask the binary signal m. $\beta(m)$ can be described as:

$$\beta(m) = \begin{cases} \beta_0 & \text{if } m = 0 \\ \beta_1 & \text{if } m = 1 \end{cases} \tag{2.22}$$

β_1 and β_0 are selected such that the condition of (2.4) is met, sufficiently different to prevent noise and parameter uncertainty extraction errors, and within a neighborhood as not to dramatically change the characteristics of the transmitted state signal. The synchronization error Φ_{sync} can be described as:

$$\Phi_{sync} = \begin{bmatrix} \Phi_1 \\ \Phi_2 \\ \Phi_3 \end{bmatrix} \tag{2.23}$$

$$\begin{aligned} \Phi_1 &= x_1 - z_1 \\ \Phi_2 &= x_2 - z_2 \\ \Phi_3 &= x_3 - z_3 \end{aligned}$$

As such the time derivative of the synchronization error states while $m = 0$ are:

$$\begin{aligned}
\dot{\Phi}_1 &= \dot{x}_1 - \dot{z}_1 \\
&= \sigma(\Phi_2 - \Phi_1) \\
\dot{\Phi}_2 &= \dot{x}_2 - \dot{z}_2 \\
&= \beta_0 x_1 - x_3 x_1 - x_2 - \beta_0 x_1 + z_3 x_1 + z_2 \\
&= -(x_2 - z_2) - (x_3 - z_3)x_1 \\
&= -\Phi_3 x_1 - \Phi_2 \\
\dot{\Phi}_3 &= \dot{x}_3 - \dot{z}_3 \\
&= x_1 x_2 - \rho x_3 - x_1 z_2 + \rho z_3 \\
&= (x_2 - z_2)x_1 - \rho(x_3 - z_3) \\
&= \Phi_2 x_1 - \rho\Phi_3
\end{aligned} \tag{2.24}$$

A Lyapunov function, $V(\Phi)$, similar to that shown by Cuomo and Oppenheim, can be selected to show asymptotic stability of the synchronization error Φ_{sync} when the message $m = 0$.

$$V(\Phi) = \frac{1}{\sigma}\Phi_1^2 + \frac{1}{2}\Phi_2^2 + \frac{1}{2}\Phi_3^2 \tag{2.25}$$

$$\begin{aligned}
\dot{V}(\Phi) &= \frac{2}{\sigma}\Phi_1\dot{\Phi}_1 + \Phi_2\dot{\Phi}_2 + \Phi_3\dot{\Phi}_3 \\
&= 2(\Phi_2 - \Phi_1)\Phi_1 + (-\Phi_3 x_1 - \Phi_2)\Phi_2 + (\Phi_2 x_1 - \rho\Phi_3)\Phi_3 \\
&= 2\Phi_1\Phi_2 - 2\Phi_1^2 - \Phi_2^2 - \rho\Phi_3^2 \\
&= -(\Phi_1 - \Phi_2)^2 - \Phi_1^2 - \rho\Phi_3^2
\end{aligned} \tag{2.26}$$

Global asymptotic stability is shown when $m = 0$. Equation (2.25) is positive definite and radially unbounded and equation (2.26) is negative definite. Further more it can

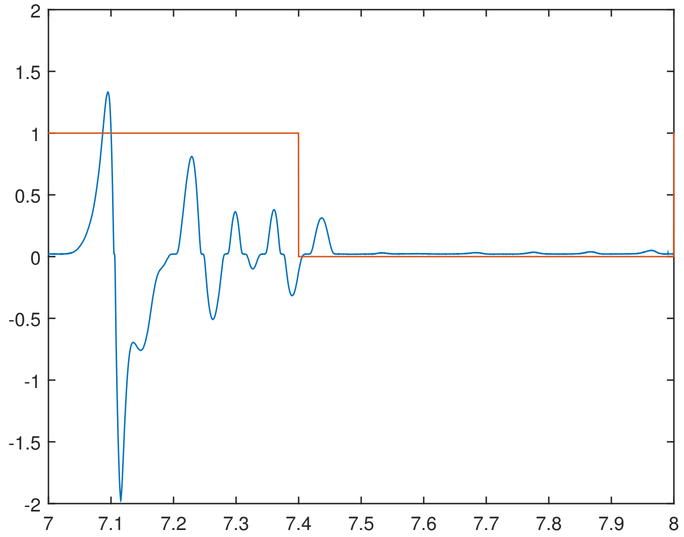


Figure 2.2: A plot of $x_1 - z_1$ vs the message m for a double alternating bit space in real circuitry

be shown that when $m = 1$ the time derivative of the synchronization error becomes:

$$\begin{aligned}
\dot{\Phi}_1 &= \sigma(\Phi_2 - \Phi_1) \\
\dot{\Phi}_2 &= \dot{x}_2 - \dot{z}_2 \\
&= \beta_1 x_1 - x_3 x_1 - x_2 - \beta_0 x_1 + z_3 x_1 + z_2 \\
&= (\beta_\Delta - \Phi_3) x_1 - \Phi_2 \\
\dot{\Phi}_3 &= \Phi_2 x_1 - \rho \Phi_3
\end{aligned}$$

Where

$$\beta_\Delta = \beta_1 - \beta_0$$

It is apparent from $\dot{\Phi}_2 = (\beta_\Delta - \Phi_3)x_1 - \Phi_2$ that the coordinate corresponding to synchronization, $\Phi_{sync} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}^T$, is no longer an equilibrium for the system. The effect of this synchronization error mismatch relative to the message m is shown in

Figure 2.2. It is also important to note that from (2.20) and the leading derivation from Swinnerton-Dyer that the two mismatched systems are both bounded, as such Φ_{sync} will also be bounded.

2.3 Cryptanalysis and Security

Dynamic chaotic encryption techniques offer a simple mathematical method of encryption that can be implemented in real-time with analog circuitry and minimal processing power. Cuomo and Oppenheim (1993) have implemented the CSK system in circuitry, yet commercial CSK encryption equipment is not widely available. The CSK system itself unfortunately is not secure. This section will explore the techniques available to crack and defeat the security of the CSK system.

2.3.1 The Return Map Attack

The return map (RM) attack is a method of monitoring the transmitted state's local minimum and maximum points to distinguish changing system characteristics. Pérez and Cerdeira pioneered this encryption breaking technique. The method is based off of the observations of Lorenz that a single state can be used to produce a return map with dynamics that tend towards a one dimensional set.

Pérez and Cerdeira describes the construction of the RM from the nth local maximum and local minimum of the first or second state of (2.1), denoted as $\overline{X}_n$ and $\overline{Y}_n$ respectively. The RM is composed of a comparison of functions:

$$\begin{aligned} A_n &= \overline{X}_n + \overline{Y}_n \\ B_n &= \overline{X}_n - \overline{Y}_n \end{aligned} \tag{2.27}$$

Pérez and Cerdeira also describes an additional set of functions that result in an identical RM due to the symmetric nature of the Lorenz system. Plotting B_n vs A_n yields the RM, of which three lines form. One manner to describe this map is to

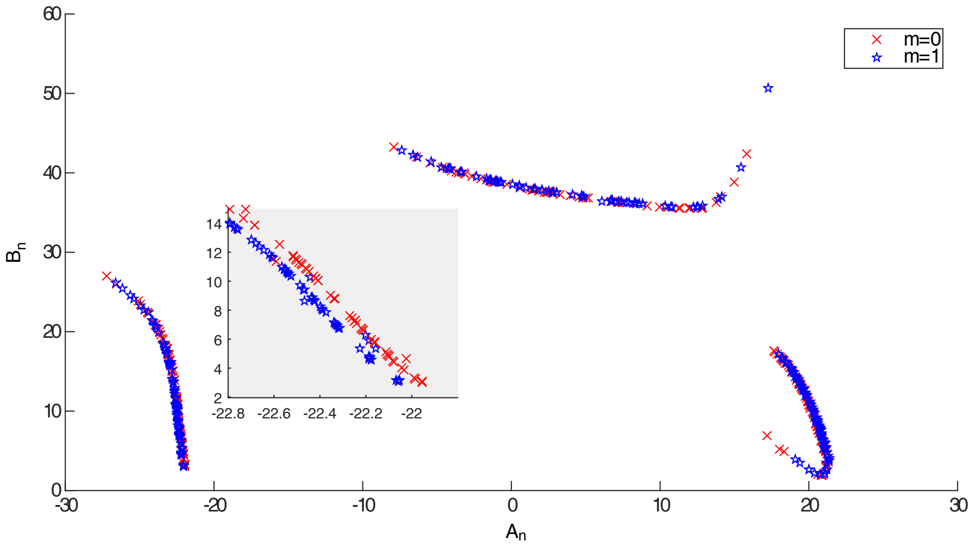


Figure 2.3: The Return Map calculated from the x output state using the CSK encryption technique.

correlate how the succeeding local minimum and maximum relate to the foci. Referencing Figure 2.1 with the state x from (2.1) being on the horizontal axis and y on the vertical, and using x as the transmitted state. When x is a local maximum it can only be:

$$\begin{cases} a & x{>}\sqrt{\rho(\beta-1)} \\ b & 0 > x{>} -\sqrt{\rho(\beta-1)} \end{cases}$$

When x is a local minimum

$$\begin{cases} a' & x{<} -\sqrt{\rho(\beta-1)} \\ b' & 0 < x{<}\sqrt{\rho(\beta-1)} \end{cases}$$

From this B_n can be deduced to have three distinct possibilities in region, which Figure 2.3 clearly shows. A region that correlates to a transition from one focus to the other, in this instance A_n on average will be towards 0 and between $\pm\sqrt{\rho(\beta-1)}$,

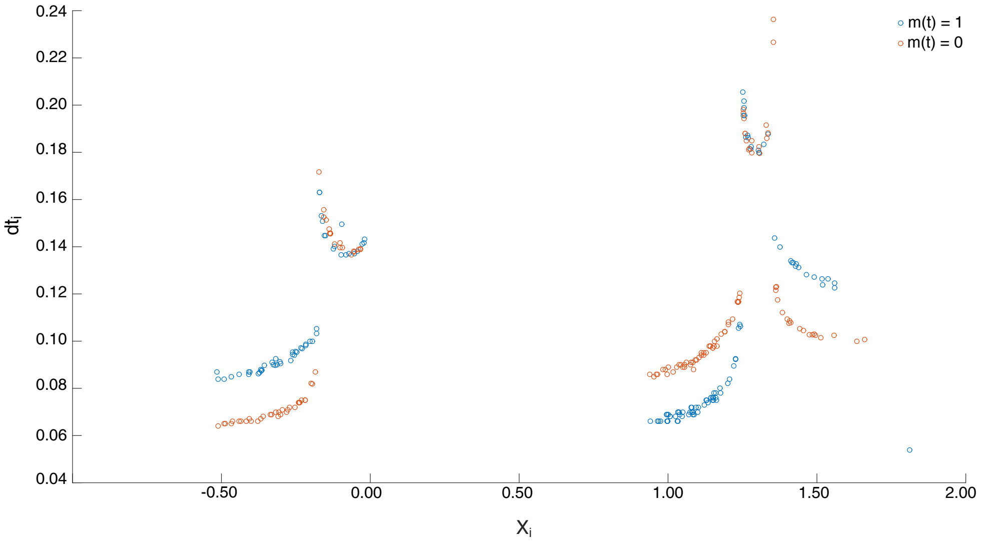


Figure 2.4: The Return Time Map calculated from the x output state using a simple switch TS-CSK encryption technique.

and B_n will be at it's largest value. The other instances are then those minimum and maximums that occur and the trajectory travels about the two foci.

The CSK method described in (2.21), which relies on direct parameter modulation to encrypted the data either through the parameter β or ρ will always be vulnerable to the RM attack. The CSK method obviously changes the foci based on which bit is present and as such distorts the dynamics of the system enough that a RM vulnerability is made evident (Yang et al., 1998).

2.3.2 Return Time Map Attack

As will be described in Section 2.4 the RM attack can easily be defeated by performing the encryption modulation in a time-scaling factor. One might consider than how this time scaling factor will affect the peaks and time distance of peaks of the transmitted signal. This method of examining the peak changes in time is the Return Time Map (RTM) attack (Candaten and Rinaldi, 2000). An example RTM can be seen in Figure 2.4. Obviously a time-scaling factor that has only a switching event that occurs at bit changes would be detectable just by observation of the transmitted state for significant changes. The RTM is not necessary in this instance, but as Figure 2.4 shows a RTM can be useful in the instance that simple false switching events occur. The RTM in Figure 2.4 is applied to a time scaled CSK system with a false switching event around the origin of the second state $x_2(t)$. To perform the RTM attack, a map is constructed by monitoring only the local maximums, X_i, and the time between them, $dt_i = t_{i+1} - t_i$. Where X_i is the i^{th} local maximum and t_i is the time that the i^{th} local maximum occurs.

2.4 Time Scaling Factor

To overcome the security weakness of the CSK system to the RM attack, the encryption of the plain-text message $m(t)$ can be handled instead by a ”time scaling function” $\lambda(x(t), m)$. If one is to consider any autonomous dynamical system:

$$\frac{d}{dt}x = f(x) \tag{2.28}$$

With a time scaling function:

$$\begin{aligned} \frac{dt}{d\tau} &= \lambda(x) && (2.29) \\ \tau(t_0) &= \tau_0 \\ 0 < \lambda(x) &< \infty && (2.30) \end{aligned}$$

It’s clear that then:

$$\frac{d}{d\tau}x = \lambda(x)f(x) \tag{2.31}$$

Condition (2.30) implies that the new time τ is strictly monotone and increasing with respect to time t (Sampei and Furuta, 1986). The result of (2.31) clearly also shows that the function $\lambda(x)$ does not change the phase space of x in respect to its attractors or equilibriums. This time scaling factor then does not distort the trajectory of x other than changing the time at which it takes to complete or reach a certain value (Materassi and Basso, 2008). Clearly if the message $m(t)$ is encoded then within a time-scaling factor, the RM attack can be defeated through its dependency on a change in state phase space.

2.4.1 Time Scaling Chaotic Shift Keying

To apply this time-scaling factor to a Lorenz based chaotic system, creating a Time Scaling Chaotic Shift Keying (TS-CSK) encryption system, a function $\lambda(x, m)$ is selected. The resulting system can then be described as:

$$\begin{aligned} \dot{x}_1 &= \sigma(x_2 - x_1)\lambda(x, m) & \dot{z}_1 &= \sigma(z_2 - z_1)\lambda(z, 0) \\ \dot{x}_2 &= \big((\beta - x_3)x_1 - x_2\big)\lambda(x, m) & \dot{z}_2 &= \big((\beta - z_3)x_1 - z_2\big)\lambda(z, 0) \\ \dot{x}_3 &= (x_1x_2 - \rho x_3)\lambda(x, m) & \dot{z}_3 &= (x_1z_2 - \rho z_3)\lambda(z, 0) \end{aligned} \tag{2.32}$$

$$\lambda(x, m) = \begin{cases} \lambda_m & \delta(x) = 0 \\ \lambda_{1-m} & \delta(x) = 1 \end{cases} \tag{2.33}$$

Where $\delta(x)$ is considered the decision engine. From a security standpoint, the decision engine should be chosen such that the switching event of $\lambda(x, m)$ cannot be deciphered from the transmitted signal. Several possibilities for $\delta(x)$ exist. Materassi and Basso (2008), of which this work is a continuation of, describes a $\delta(x)$ as:

$$\delta(x) = \begin{cases} 0 & \frac{v^T x}{h} \text{ is even} \\ 1 & \frac{v^T x}{h} \text{ is odd} \end{cases} \tag{2.34}$$

Where the unitary selection vector v is:

$$v = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}$$

However this decision engine becomes increasingly difficult and expensive to implement the faster the Lorenz system oscillates. A initial decision engine was conceived that simplified the multiple alternating regions to just two regions:

$$\delta(x) = \begin{cases} 0 & v^T x < 0 \\ 1 & v^T x \geq 0 \end{cases} \tag{2.35}$$

The decision engine described by (2.34) was found by Materassi and Basso (2008) to be secure from both the RM attack and the RTM attack. The RM is defeated because the TS-CSK encryption method does not modify the underlying Lorenz function in respect to its orbital foci. Further, the TS-CSK method described by (2.32) is secure against a RM attack for any selection of $\delta(x)$ that leaves the underlying Lorenz system chaotic.

Immunity to the RTM however requires that the time difference between orbits not be significantly determined by the message $m(t)$. The even-odd scheme devised by Materassi and Basso (2008) has adequate switching events between bit changes that the RTM becomes obfuscated such that RTM based bit extraction is not possible. This property does not hold true for a decision engine employed by the plus-minus TS-CSK (PM TS-CSK) system (2.35) with a reasonable time difference between bits. A slightly more complex decision engine was conceived.

$$\delta(x) = \begin{cases} \delta_z & x_2(t) < -\sqrt{\rho(\beta-1)} \\ 1-\delta_z & -\sqrt{\rho(\beta-1)} \leq x_2(t) < 0 \\ \delta_z & 0 \leq x_2(t) < \sqrt{\rho(\beta-1)} \\ 1-\delta_z & x_2(t) \geq \sqrt{\rho(\beta-1)} \end{cases} \tag{2.36}$$

Where:

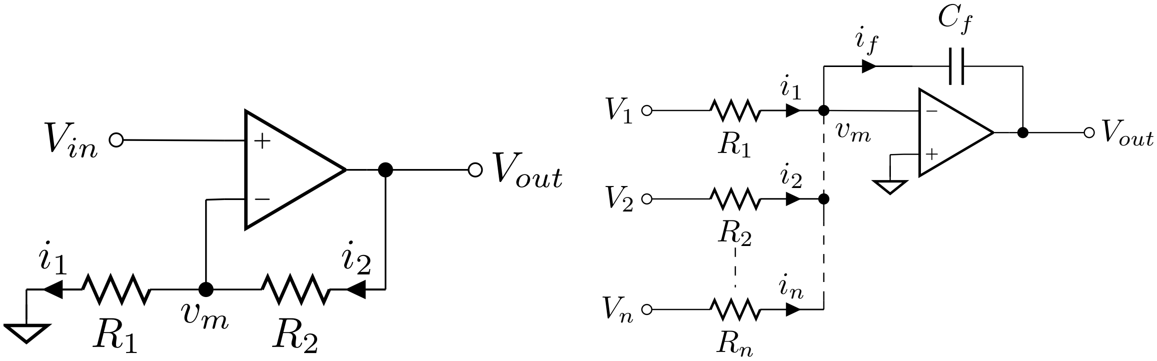
$$\delta_z = \begin{cases} 1 & x_3(t) \geq \beta - 1 \\ 0 & x_3(t) < \beta - 1 \end{cases} \tag{2.37}$$

This new decision engine sets the regions of operation and switching about the equilibrium of the system. A switch occurs when the third dynamic $x_3(t)$ crosses from one side of its equilibrium to another. To add more regions of operation, the system splits the second dynamic into 4 regions; the region below the negative focus, the region between the negative focus and the origin, the region from the origin to the positive focus, and finally region above the positive focus. (2.36) and (2.37) form the 8-section TS-CSK system.

The synchronization of the system (2.32) can again be expressed using the same Lyapunov function from (2.25) with the same error function Φ_{sync} as described in (2.23). The time derivative of Φ_{sync} while the message $m(t) = 0$ now becomes:

$$\begin{aligned} \dot{\Phi}_1 &= \sigma\Big(\lambda(x)(x_2 - x_1) - \lambda(z)(z_2 - z_1)\Big) \\ \dot{\Phi}_2 &= \Big(\beta\big(\lambda(x) - \lambda(z)\big) + \big(\lambda(z)z_3 - \lambda(x)x_3\big)\Big)x_1 + \lambda(z)z_2 - \lambda(x)x_2 \\ \dot{\Phi}_3 &= \Big(\lambda(x)x_2 - \lambda(z)z_2\Big)x_1 + \rho\Big(\lambda(z)z_3 - \lambda(x)x_3\Big) \end{aligned} \tag{2.38}$$

The case of interest is when the time scaling factor of both systems is equal, $\lambda(x) = \lambda(z)$. While the message $m(t) = 0$ this will occur while x and z are within the



(a) Non-Inverting Operational Amplifier **(b)** Inverting Integrator Operational Amplifier

Figure 2.5: Basic Operational Amplifier Circuits

same operation region. In the case that $\lambda(x) = \lambda(z)$, (2.38) will become similar to (2.24), and the Lyapunov equation indicates asymptotic stability about the point $\Phi_{sync} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}^T$. Of course, the two systems will not always be operating in a region such that $\lambda(x) = \lambda(z)$, however due to the cyclic nature of the chaotic system, as well the property of the time-scaling factor to not change the phase space, the regions of $\lambda(x) \neq \lambda(z)$ are periodic while there is no synchronization. It should also be noted that the time at which the transmitter system trajectory transverses the region that causes $\lambda(x) \neq \lambda(z)$ will inherently be different from that of the receiver system. The lack of synchronization when $m(t) = 1$ is obvious, as for $\lambda(x) = \lambda(z)$ to hold true, x and z will be operating in adjacent regions. Once x and z enter the same region $\lambda(x) \neq \lambda(z)$ and synchronization will not occur.

2.5 Operational Amplifier Circuits

The operational amplifier can be described by an ideal model where the voltage at both inputs (non-inverting + and inverting −) is forced to be equal by the output when in closed-loop configuration, additionally no current flows in or out of the inputs (Horowitz and Hill, 1983). The operating principle of the circuits described in chapter 3 are assumed to be near ideal.

2.5.1 The Non-Inverting Gain

Figure 2.5a describes the topology of a non-inverting amplifier (DeCarlo and Lin, 1994). The system is described by:

$$\begin{aligned}
v_m &= V_{in} \\
i_1 &= i_2 \\
&= \frac{v_m}{R_1} \\
&= \frac{V_{out} - v_m}{R_2} \\
\frac{V_{in}}{R_1} &= \frac{V_{out} - V_{in}}{R_2} \\
V_{out} &= \left(1 + \frac{R_2}{R_1}\right) V_{in} \qquad (2.39)
\end{aligned}$$

2.5.2 Inverting Integrator

Figure 2.5b describes a summing inverting operation amplifier (Texas Instruments, 2004).

$$\begin{aligned}
i_f &= i_1 + i_2 + \ldots + i_n \\
i_i &= \frac{V_i}{R_i} \\
V_{out} &= -\int \frac{i_f}{C_f}\,\mathrm{dt} \\
&= -\frac{1}{C}\int \left(\frac{V_1}{R_1} + \frac{V_2}{R_2} + \ldots + \frac{V_n}{R_n}\right)\mathrm{dt} \qquad (2.40)
\end{aligned}$$

Chapter 3

Practical Implementation and Simulation

For practical implementation of the Lorenz system as an encryption device, simulations parameter, tuning and performance testing are completed. This chapter will detail the steps and manners in which all methodology was completed. Performance metrics shall be detailed as to ascertain the security and practicality of the encryption system. Hardware configuration and selection shall be detailed. The base Lorenz system described in this section uses the form:

$$\begin{aligned}\dot{x} &= k\sigma(y - x)\\ \dot{y} &= k((\beta - z)x - y)\\ \dot{z} &= k(xy - \rho z)\end{aligned}$$

Where k is a constant time-scaling factor. The parameters selected are:

$$
\begin{aligned}
k &= 100 \\
\sigma &= 10 \\
\beta &= 25.6 \\
\rho &= 2
\end{aligned}
\tag{3.1}
$$

The modulation values can be described as:

$$
\begin{aligned}
\beta(m) &= \begin{cases} \beta_0 = & 60.5 \\ \beta_1 = & 60 \end{cases} \\
\lambda(q, m) &= \begin{cases} \lambda_0 = & \frac{23}{26} \\ \lambda_1 = & \frac{23}{20} \end{cases}
\end{aligned}
\tag{3.2}
$$

3.1 Numerical Simulations

Numerical simulations were calculated using MATLAB and Simulink. The solver ode45 was used in Simulink with a relative tolerance of 10^{-12}.

3.1.1 CSK Simulation

The CSK system was modeled in Simulink, and is described by the block diagrams in Figure 3.1 and Figure 3.2. Figure 3.1 represents the encryption transmitter design. The block labeled β_m was implemented using a simple set of math functions such that:

$$\beta_m = (\beta_1 - \beta_0)m(t) + \beta_0$$

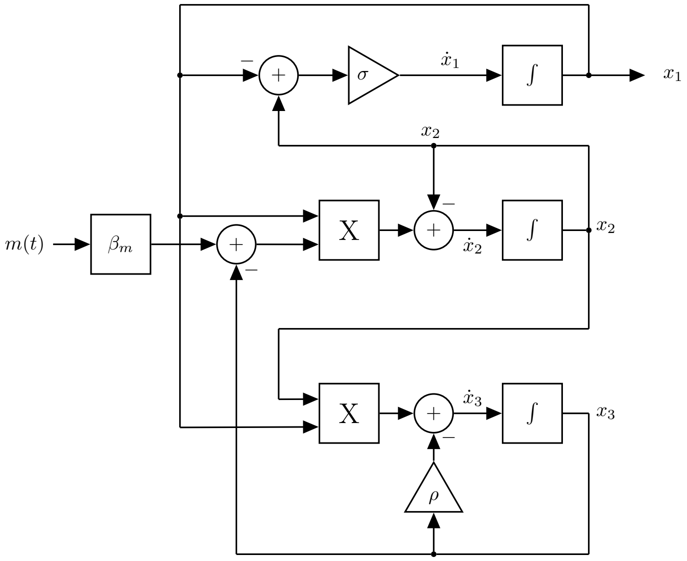


Figure 3.1: Block diagram of the transmitter for the CSK system

Initial conditions for the system are set as:

$$x_0 = \begin{bmatrix} x_{1_0} \\ x_{2_0} \\ x_{3_0} \end{bmatrix}$$

The receiver system in Figure 3.2 is implemented with the modulating constant set to β_0. To allow testing of system robustness to noise a band-limited Gaussian noise η is added into the transmitted state x_1. Initial conditions for the receiver system are set as:

$$z_0 = \begin{bmatrix} z_{1_0} \\ z_{2_0} \\ z_{3_0} \end{bmatrix}$$

A synchronization test output is then computed in simulation to yield:

$$\Phi_1^2 = (x_1 - z_1)^2 \tag{3.3}$$

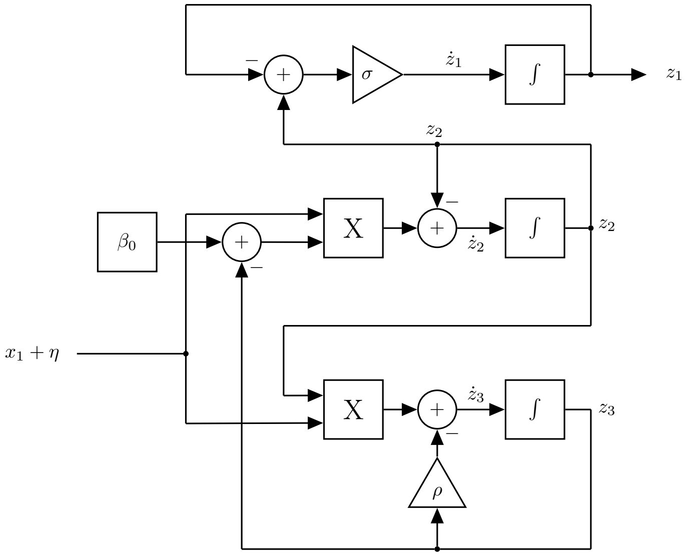


Figure 3.2: Block diagram of the receiver for the CSK system

The result of (3.3) is then further refined outside of the Simulink simulation using a MATLAB script described in Section 3.1.3.

3.1.2 TS-CSK simulation

The TS-CSK Simulink block diagram describing the transmitter and receiver are seen in Figure 3.3 and Figure 3.4, respectively. The initial conditions for the system are set by:

$$x_0 = \begin{bmatrix} x_{1_0} \\ x_{2_0} \\ x_{3_0} \end{bmatrix} \quad z_0 = \begin{bmatrix} z_{1_0} \\ z_{2_0} \\ z_{3_0} \end{bmatrix}$$

The function $\lambda(x, m)$ in both the transmitter and receiver is described in equation (2.33). In the instance of the receiver $\lambda(z_2, 0)$ is used. A band-limited Gaussian noise η is added to the transmitted state x_1 before entering the receiver to test the systems robustness to line noise.

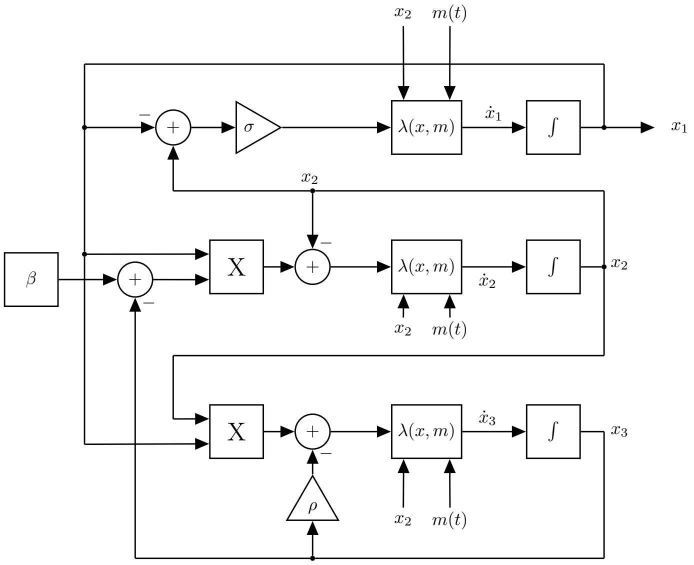


Figure 3.3: Block diagram of the transmitter for the TS-CSK system

As with the CSK system a synchronization test as described in (3.3) is saved for later refinement and message extraction.

Message Structure

The message is structured in a manner to decrease the number of incorrectly extracted bits. Between each bit a padding section is added as a percentage (∇) of overall message frequency such that:

$$\bar{m}(t) = \begin{cases} m(t) & \text{if } t \leq T_t \\ 0 & \text{if } t > T_t \end{cases}$$

Where $m(t)$ is the full bit width message with period T and:

$$T_t = T(\text{floor}(\frac{t}{T})) + \nabla T$$
$$0 \leq \nabla \leq 1$$

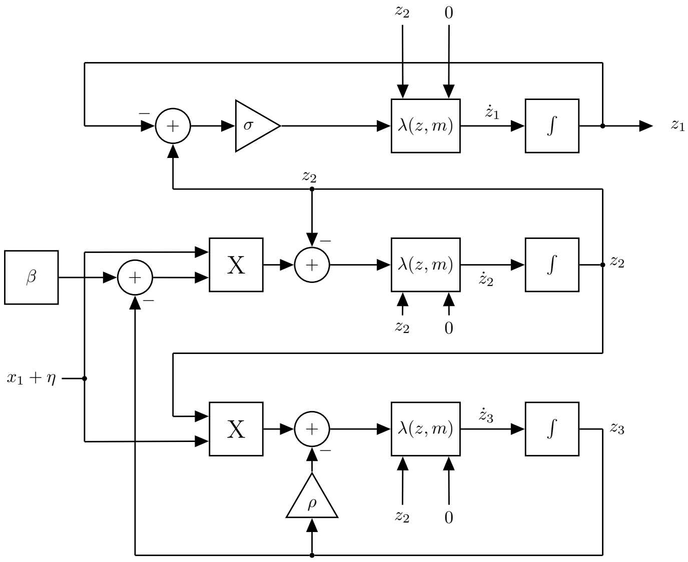


Figure 3.4: Block diagram of the receiver for the TS-CSK system

3.1.3 Message Extraction

The message extraction technique uses a periodic averaging approach with a threshold decision. Once a decision is made for each potential bit this information is then tested against $m(t)$ as used in the simulation. This approach requires a previous knowledge of the expected message frequency. A threshold level must be selected such that all bits are able to be extracted accurately, in the experimental testing this value is selected through a range to yield the best results.

The periodic averaging can be expressed as:

$$\psi(t) = \frac{1}{T}\int_{\tau_0}^{\tau_1} \varphi(n)\text{sync}(n)dn \tag{3.4}$$

$$m_r(t) = \begin{cases} 1 & \psi(t) \geq \chi \\ 0 & \psi(t) < \chi \end{cases} \tag{3.5}$$

Where $\varphi(n)$ is a weighting function, χ is the threshold, and:

$$\tau_0 = T(\text{floor}(\frac{t}{T}))$$
$$\tau_1 = \tau_0 + T$$

The weighting function used in this work can be described as:

$$\varphi(n) = \begin{cases} 0.5 & n < \tau_0 + (1-w)\Delta\tau \\ 1 & n > \tau_0 + w\Delta\tau \\ 2 & \text{otherwise} \end{cases} \tag{3.6}$$

3.1.4 Bit Error Detection and Testing

To test the system accuracy the message extracted is tested against the original signal $m(t)$. The padding added to form $\bar{m}(t)$ is ignored for simplicity. The error in bit detection is described as the bit error rate (BER). It is calculated as:

$$BER = \frac{1}{N}\sum_{n=0}^{N-1} g(n)$$

Where

$$g(n) = \begin{cases} 0 & \text{if } \bar{m}(nT + \frac{T}{2}) = m_r(nT + \frac{T}{2}) \\ 1 & \text{if } \bar{m}(nT + \frac{T}{2}) \neq m_r(nT + \frac{T}{2}) \end{cases}$$
$$N = \text{floor}(\frac{t_f}{T})$$
$$t_f = \text{final simulation time}$$

Message Types

To test practicality of the TS-CSK and CSK systems two methods of signals are generated. For short term testing a simple alternating bit pattern is established. This is considered to be a worse case scenario in terms of system synchronization, and is

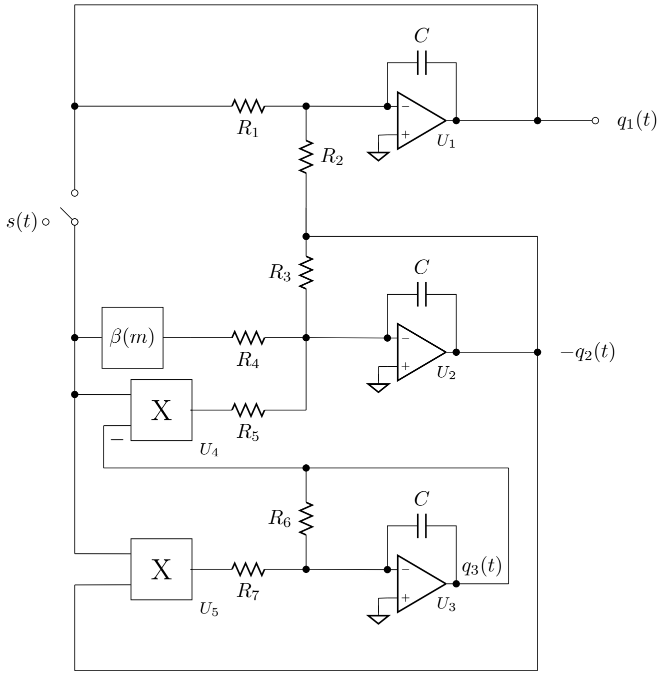


Figure 3.5: CSK system Circuit Diagram

effective for tuning maximum message frequency and internal signal parameters. For long time BER calculations an American Standard Code for Information Interchange (ASCII) text file is transcribed into a rolling bit stream. The extracted message is then also able to be saved into a text file, functioning much like an encrypted text messaging system.

3.2 Circuit Design

To implement the chaotic encryption in circuitry, operational amplifiers and specialized semi-conductor integrated circuits are used. The components chosen are

Table 3.1: Component Values of the CSK Transmitter and Receiver Circuit

Index	Value	Index	Value
R_1, R_2	100 kΩ	C	0.1 µF
R_3, R_4	1 MΩ	U_1, U_2, U_3	LT1057
R_5, R_7	8 kΩ	U_4, U_5	AD633
R_6	499 kΩ		

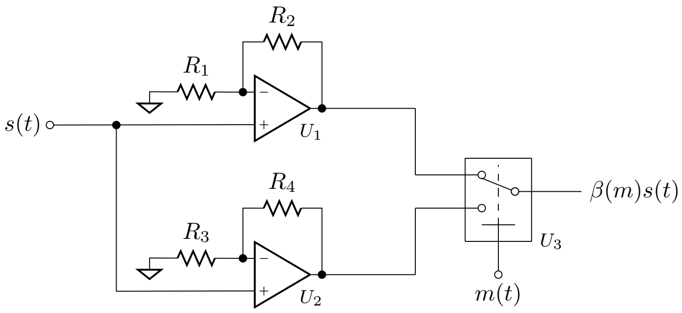


Figure 3.6: Circuit Diagram of β Modulator

configured to produce the same dynamical models as shown in equations (2.21) and (2.32). A scaling factor is utilized to keep system operation within the operating ranges of the selected hardware. The scale for this work is $100\,\mathrm{mV} = 1$. To assist in troubleshooting, circuit construction methodology and to verify the commonality between the numerical simulation and circuit simulation, the CSK system was designed. The circuit draws heavy inspiration from web published work (Horowitz, 2016). The CSK transmitter and receiver designs can be seen in Figure 3.5.

The CSK system components are selected such that the gains are equivalent to the parameters listed in (3.1) with the scaling factor taken into account. The component values of Figure 3.5 are listed in Table 3.1. The β modulation block (Fig. 3.6) is used for encoding the message within the encryption system. This circuit is a variable gain circuit constructed from an inverting summing amplifier and two separate inverting amplifiers, of which one is controlled by the switch U_4. The component values for the β-modulator can be seen in Table 3.2.

The capacitor C is chosen to limit the gain k and the speed of the Lorenz oscillation to improve resolution with lower cost data acquisition equipment. The

Table 3.2: Component Values of the β-Modulator Circuit

Index	Value	Index	Value
R_1, R_3	$10\,\mathrm{k\Omega}$	U_1, U_2	LT1057
R_2	$595\,\mathrm{k\Omega}$	U_3	DG419
R_4	$590\,\mathrm{k\Omega}$		

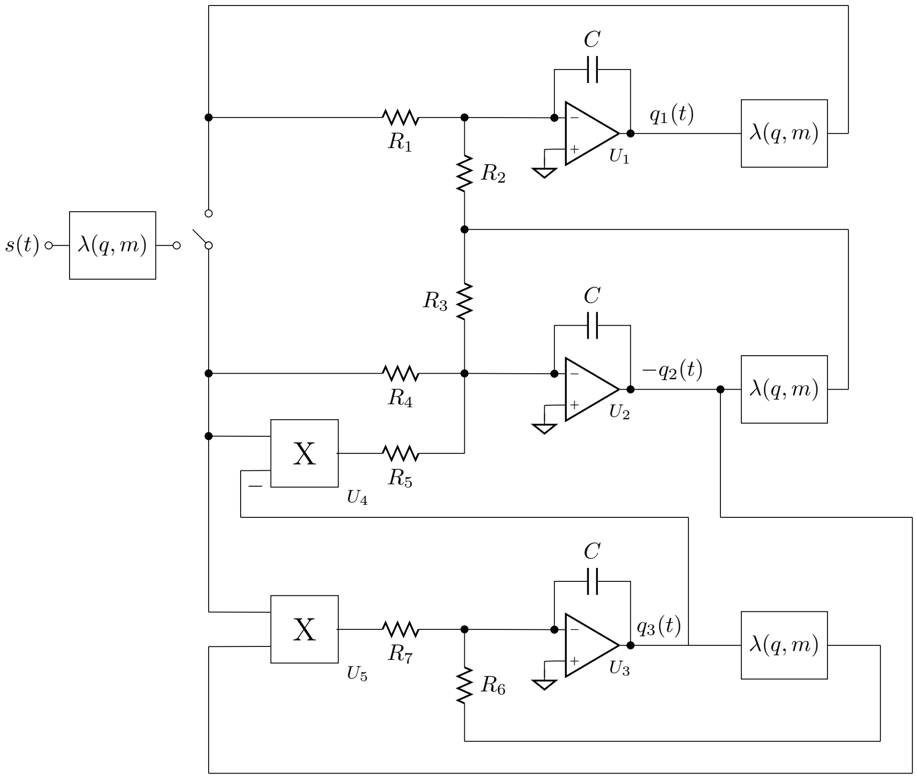


Figure 3.7: TS-CSK circuit diagram

LT1057 operational amplifier from Linear Technologies provides a good low noise fast amplification option as well as having a designated LTspice model. To handle the multiplication task the AD633 from Analog Devices Inc. was chosen. The AD633 was selected for its SPICE model availability and overall unit cost. To handle switching tasks needed within the β-modulator the Maxim Integrated DG419 single pole double throw (SPDT) analog switch was chosen. All integrated circuit choices can function off of a ±12 V DC power supply. In full circuit simulation however the DG419 model

Table 3.3: Component Values of the TS-CSK Transmitter and Receiver Circuit

Index	Value	Index	Value
R_1, R_2	100 kΩ	R_6	499 kΩ
R_3	1 MΩ	C	0.1 µF
R_4	39 kΩ	U_1, U_2, U_3	LT1057
R_5, R_7	10 kΩ		

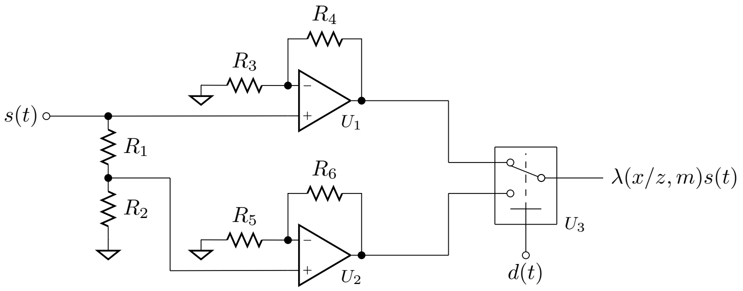


Figure 3.8: Circuit Diagram of the λ Modulator

is replaced with ideal switching options. The model for the DG419 functions perfectly in a small scale test of the β-modulator, but creates numerical singularities when used within the full Lorenz model.

The TS-CSK system as implemented in circuitry is shown in Figure 3.7. As can be seen, compared to the CSK system the TS-CSK system has added complexity and circuitry. To maintain the gains from (3.1) the components for the transmitter and receiver in Figure 3.7 are selected as shown in Table 3.3. Also to maintain similarity to the CSK system, and to reduce the neccasity for additional gates, the λ-modulation function is distributed inside of the equations. Such that (2.32) becomes:

$$\begin{aligned}\dot{q}_1 &= \sigma(\lambda(q,m)q_2 - \lambda(q,m)q_1)\\ \dot{q}_2 &= \beta g - g q_3 - \lambda(q,m)q_2\\ \dot{q}_3 &= g q_2 - \rho\lambda(q,m)q_3\end{aligned} \tag{3.7}$$

Where g is selected as either $\lambda(q,m)q_1$ or $\lambda(q,m)s$ depending on whether the system is a transmitter or receiver respectively.

The λ-modulator is a combination of two circuits, the decision engine circuit for the

Table 3.4: Component Values of the λ-Modulator Circuit

Index	Value	Index	Value
R_1, R_2	100 kΩ	R_6	76.9 kΩ
R_3, R_5	100 kΩ	U_1, U_2	LT1057
R_4	15 kΩ	U_3	DG419

8-section TS-CSK system is described in Appendix A and a binary gain shown in Figure 3.8. The PM TS-CSK decision engine circuit is also described in Appendix A. The λ-modulator variable gain block is constructed of two non-inverting operational amplifier gain paths, of which selection is set by the DG419 SPDT switch. As is inherent with the non-inverting amplifier, the gain of each amp must be $G > 1$. To meet the specifications of (3.1) a simple resistor voltage divider is used at the entrance to one of the amplifier stages. Driving the DG419 requires a pull-up resistor on the output of the logic gate circuit, this was implemented off board in the initial board configuration, the later secondary decision engine board incorporated this design feature on board. The decision engine uses a series of comparators, voltage references and logic gates to perform the λ selection. The 8-section TS-CSK decision engine circuit performs the logical operation of:

$$d(x, m, t) = \Big((\overline{A} + B\overline{C}) \oplus D\Big) \oplus \overline{m(t)}$$

Where:

$$A = \begin{cases} 0 & q_2(t) < -\sqrt{\rho(\beta - 1)} \\ 1 & q_2(t) \geq -\sqrt{\rho(\beta - 1)} \end{cases}$$

$$B = \begin{cases} 0 & q_2(t) < 0 \\ 1 & q_2(t) \geq 0 \end{cases}$$

$$C = \begin{cases} 0 & q_2(t) < \sqrt{\rho(\beta - 1)} \\ 1 & q_2(t) \geq \sqrt{\rho(\beta - 1)} \end{cases}$$

$$D = \begin{cases} 0 & q_3(t) < \beta - 1 \\ 1 & q_3(t) \geq \beta - 1 \end{cases}$$

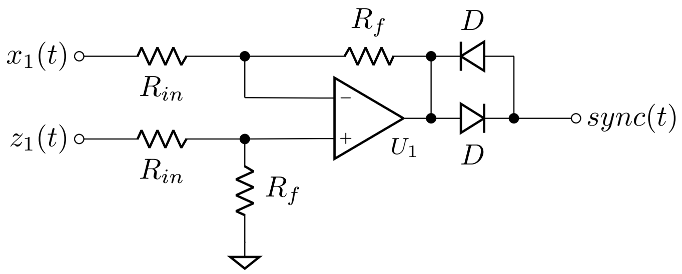


Figure 3.9: Circuit Diagram of $\Phi_1 = x_1 - z_1$

The LT1011 from Linear Technology was selected as the comparator for its LTspice model availability and performance. A 74HC00D series NAND chip was selected to provide the four NAND gates used within logic, and the 74HC266D series was chosen to perform the two XNOR operations. To create the reference points $\pm\sqrt{\rho(\beta - 1)}$ and $\beta - 1$, two LT1004-2.5 Zener diodes are used to provide steady ±2.5 V references. The desired reference points are then set via a resistor division network.

All components in the TS-CSK circuit are chosen with the best available tolerance selection to minimize gain mismatches between the transmitter and receiver circuits. All resistors are chosen to have a tolerance of 0.1%. The capacitors used in the integrator blocks are selected with a tolerance of 1.0%, with the capacitor used for comparator operation selected with a tolerance of 5.0%.

3.3 Circuit Simulation

To simulate both the CSK and TS-CSK circuits Linear Technology's LTspice IV version 4.23l was used. This simulation tool, provided free of charge by Linear Technology, contains a graphical circuit net editing tool integrated with a SPICE simulator, diagnostic tools, and graphical data rendering. The solver is configured with default settings except the alternate solver option is selected.

3.3.1 Model Parameters

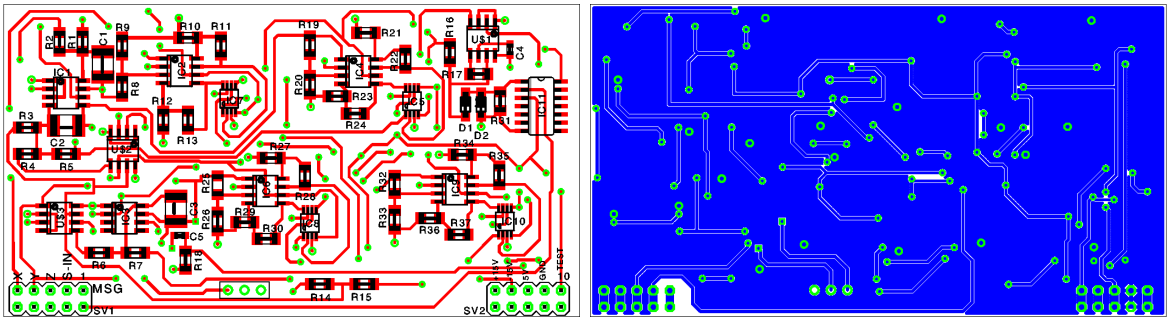
Each component was modeled using readily available SPICE models. The AD633 was implemented using a model provided by Analog Innovations (Thompson, 2016). The DG419 was modeled in initial λ-block testing with the MAX319 model from Maxim-Integrated (2017). The LT1057, LT1011A, resistor, capacitor, diode and source models are selected from the standard library.

3.3.2 Simulations

Initial simulations were used to tune the component parameters to obtain the desired operation in conjunction with following the parameter guidelines of Section 2.1. This was done by comparing $\Phi_1 = x_1 - z_1$ with the message signal. The message used was an alternating bit pattern to simulate the worst case switching scenario. The message was also tuned in frequency to provide a reasonable data transfer rate and to reduce errors present in Φ_1 as well as take into account limitations in available data acquisition equipment.

Once circuit values were configured, longer runs were completed and the output data saved. The output data for both the CSK and TS-CSK were imported into the MATLAB environment and the RTMs calculated. Due to the duration of simulation times and machine memory limitations, BERs were not calculated for the simulated circuitry.

To ensure real world reliability and function, a Monte-Carlo simulation was ran for the TS-CSK system. Each component was specified to its nominal value with the part tolerance included. The input message signal was configured as one period high and two periods low to monitor system synchronization.



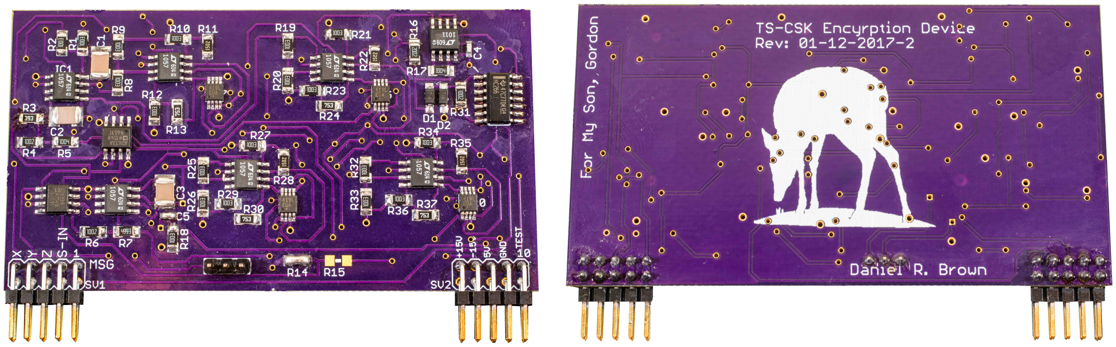
(a) Top Layer of circuit board **(b)** Bottom Layer of circuit board

Figure 3.10: Gerber view of the TS-CSK system PCB

3.4 Practical Implementation

The practical implementation and construction of the system is described in this section. The physical construction is designed with electronic breadboard compatibility in mind. Due to the need for high precision components and the shear volume of components, surface mount devices (SMD) were used. To implement SMD components with electronic breadboard, custom printed circuit boards (PCB) were designed.

To verify that the chosen hardware configuration functioned as expected, a single Lorenz system circuit was constructed using through-hole components. The resulting circuit was cumbersome in breadboard real estate usage, however was useful in proving the proper operation of the base Lorenz system in circuitry. The λ-block was then also configured using a breadboard circuit to verify continued function of the Lorenz system. After confirmation of component choice and function, a multiple purpose PCB was designed. The PCB trace, hole and component layout can be seen in Figure 3.10. This PCB is designed with a three pin header for a selection of either $v = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}^T$ or $v = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}^T$ for use with the less secure method of two region switching. The resistors R_{14} and R_{15} as seen in Figure 3.10a at the bottom center of the board, are used in coordination as a solderable jumper selection for either transmitter or receiver operation. This can be seen in Figure 3.11a as R_{14} is solder



(a) Top Layer of circuit board

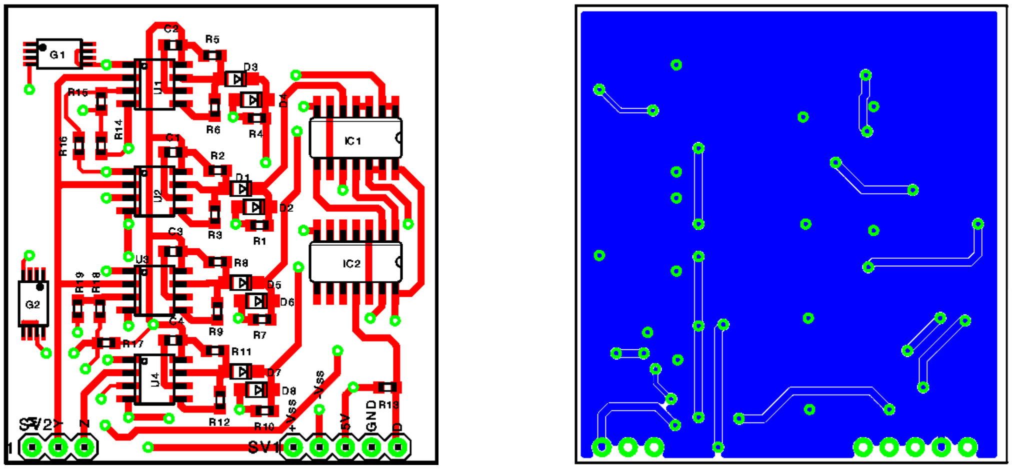
(b) Bottom Layer of circuit board

Figure 3.11: Photograph of the constructed TS-CSK system PCB

bridged, indicating a transmitter configuration. It should be noted that a 0603 size C_5 can be seen in both Figure 3.10a and Figure 3.11a, this place is left to allow for the addition of a capacitor to form a high pass filter before the on board comparator.

Initial testing and troubleshooting revealed the necessity of a pull-up resistor on the output of the last logic gate before the system of switches, this resistor was not included on the initial board. This oversight was due to the use of a different logic gate in breadboard testing. Once single board operation was verified, a second board was added to the breadboard. The transmitter and receiver were then coupled. A message $m(t)$ is created by a digital output of an Arduino NANO. The frequency and bit padding of the message $m(t)$ is set through a custom Universal Asynchronous Receiver/Transmitter (UART) protocol.

This initial board, the dynamics board, as seen in Figure 3.11 incorporates a simple decision engine that performs the decision from (2.33). This decision engine is located in the upper right hand corner of Figure 3.11a, and is comprised of U_1 and IC_{11}. The decision engine of (2.33) leaves the encryption system highly vulnerable to a RTM and as such a more complicated decision engine was designed. The Gerber board layout can be seen in Figure 3.12. The board construction is designed such that the 5-pin connector directly interfaces with the right most connector of Figure 3.11a. To save on board cost, the signal input connection of the decision engine board was



(a) Top Layer of circuit board

(b) Bottom Layer of circuit board

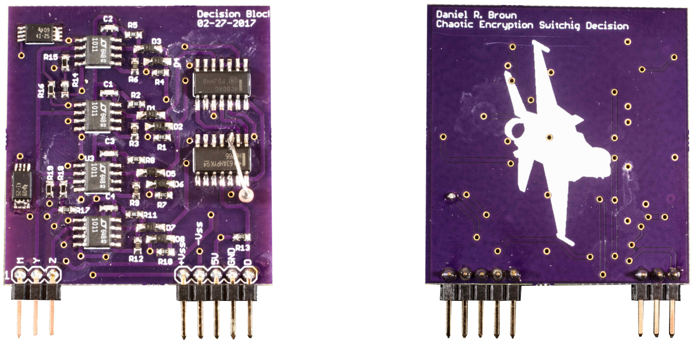
Figure 3.12: Gerber Layout of Decision Engine PCB

not extended to reach the second state 5-pin connector of the dynamics board. The connection to incorporate $q_2(t)$ and $q_3(t)$ is implemented on the breadboard. To allow the decision engine and dynamics board to interface together IC_{11} is removed from the dynamics board. The decision engine was designed to incorporate the pull-up resistor for the gate output. The constructed decision engine board can be seen in Figure 3.13.

To extract $\text{sync}(t) = x_1(t) - z_1(t)$, a LT1057 was set up in differential amplifier configuration. This can be seen in Figure 3.9. An anti-parallel diode couple are placed in series with the amplifier output to remove the small synchronization signal error present from resistor and gain mismatches between the transmitter and receiver.

3.5 Data Acquisition Methods

To provide both the 5 V and differential ±12 V an 480W ATX computer power supply was used, the Logisys PS480D-BK. The higher power wattage was selected such that the −12 V supply can provide up to 800 mA. The selection was also in part due to fast availability and lower price.



(a) Top Layer of circuit board

(b) Bottom Layer of circuit board

Figure 3.13: Photograph of the constructed Decision Engine PCB

The message delivery was accomplished using a Arduino NANO clone obtained from MPJA. The NANO would receive characters from a MATLAB script through the serial UART port. Through the UART port the frequency, bit padding, character and start send command could be received. The NANO can send one character (8 bits) at a time. A second pin from the NANO is used as a falling-edge trigger to synchronize the data acquisition (DAQ) device with the character being sent.

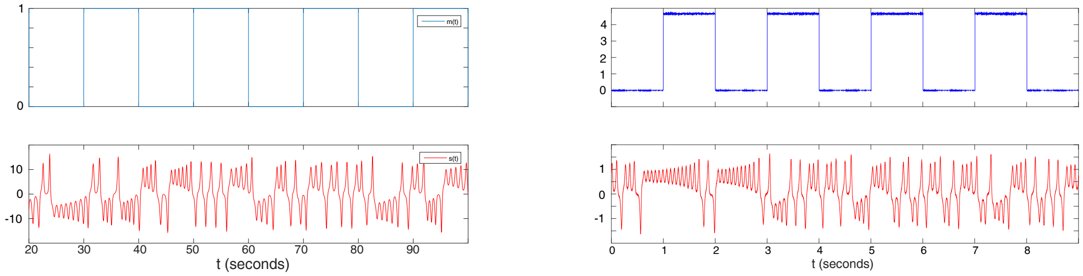
Data acquisition is accomplished using a National Instruments USB-6008 DAQ device. The device is capable of being triggered externally, has eight 12-bit single ended or differential analog inputs, and has a single channel max sample rate of 10,000 samples per second. The DC ground of the circuits, power supply, DAQ and NANO are connected in common. Data is then gathered as a single ended input. One channel collecting $\Phi_1(t)$ from the output of the diode threshold device from Figure 3.9. The second channel is used to gather the message being sent from the NANO device. Data was gathered at $5kS/s$ per channel. It should be noted that the USB-6008 does not simultaneously gather data from channels, and rather staggers point acquisitions, however this behavior was not found to have significant effect.

Chapter 4

Results

Results are acquired using the parameters listed in (3.1). The CSK and TS-CSK system use the modulating gains as described by (3.2). All graph figures were created using MATLAB and exported as Encapsulated Postscript Vector graphics (.eps) files. See appendix D for enlarged figures.

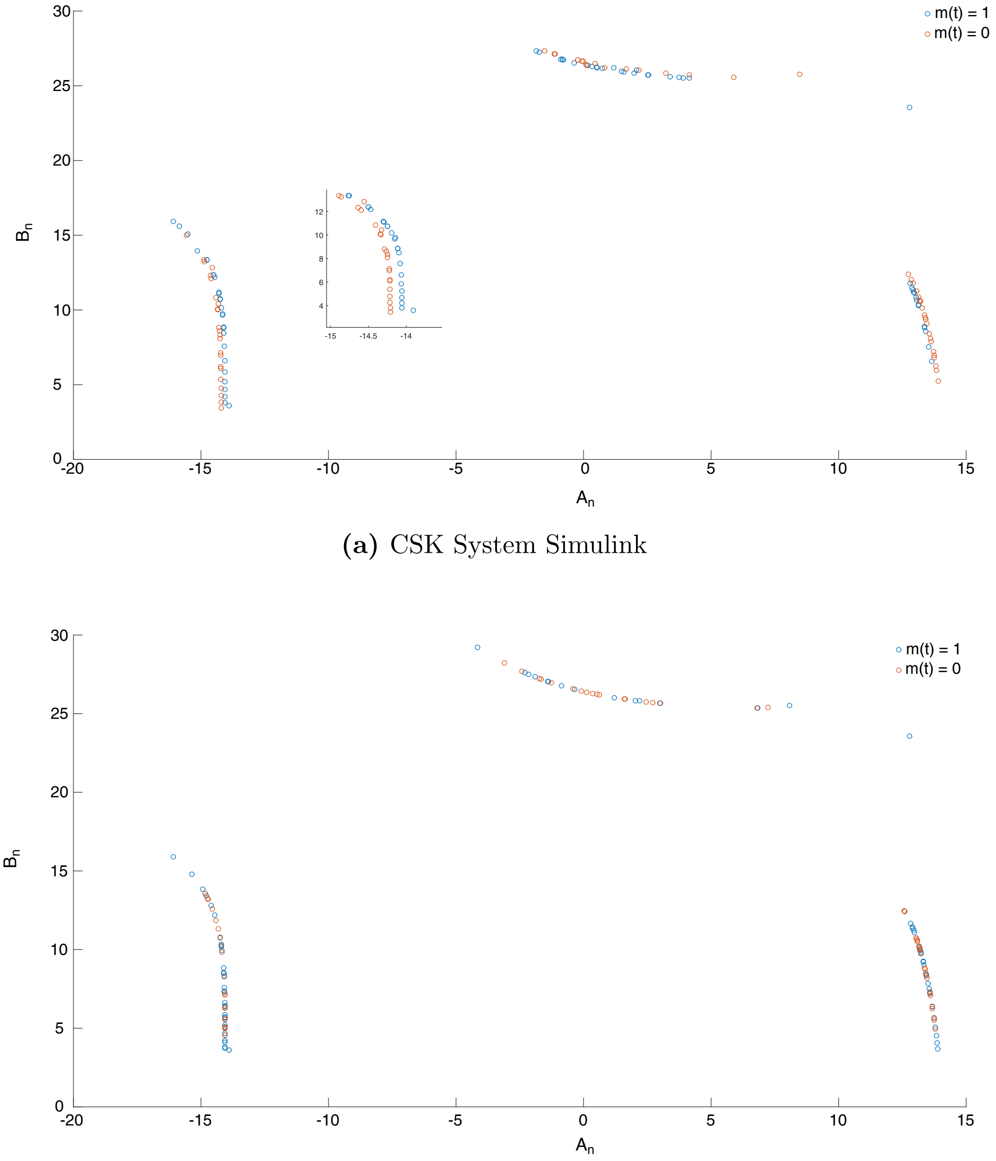
For comparison of basic pattern detection Figure 4.1 shows the response of the transmitted signal $x_1(t)$ in relation to the encrypted message $m(t)$. Figure 4.1a shows that response as simulated in the Simulink model described in Section 3.1. Figure 4.1b shows the real world data gathered including the actual $m(t)$ signal. Figures 4.2, 4.3, and 4.4 show all results for the return map (RM) attack described in Section 2.3.1. Figure 4.2a and Figure 4.2b are a comparison of RMs calculated



(a) Simulation Capture

(b) Actual Capture

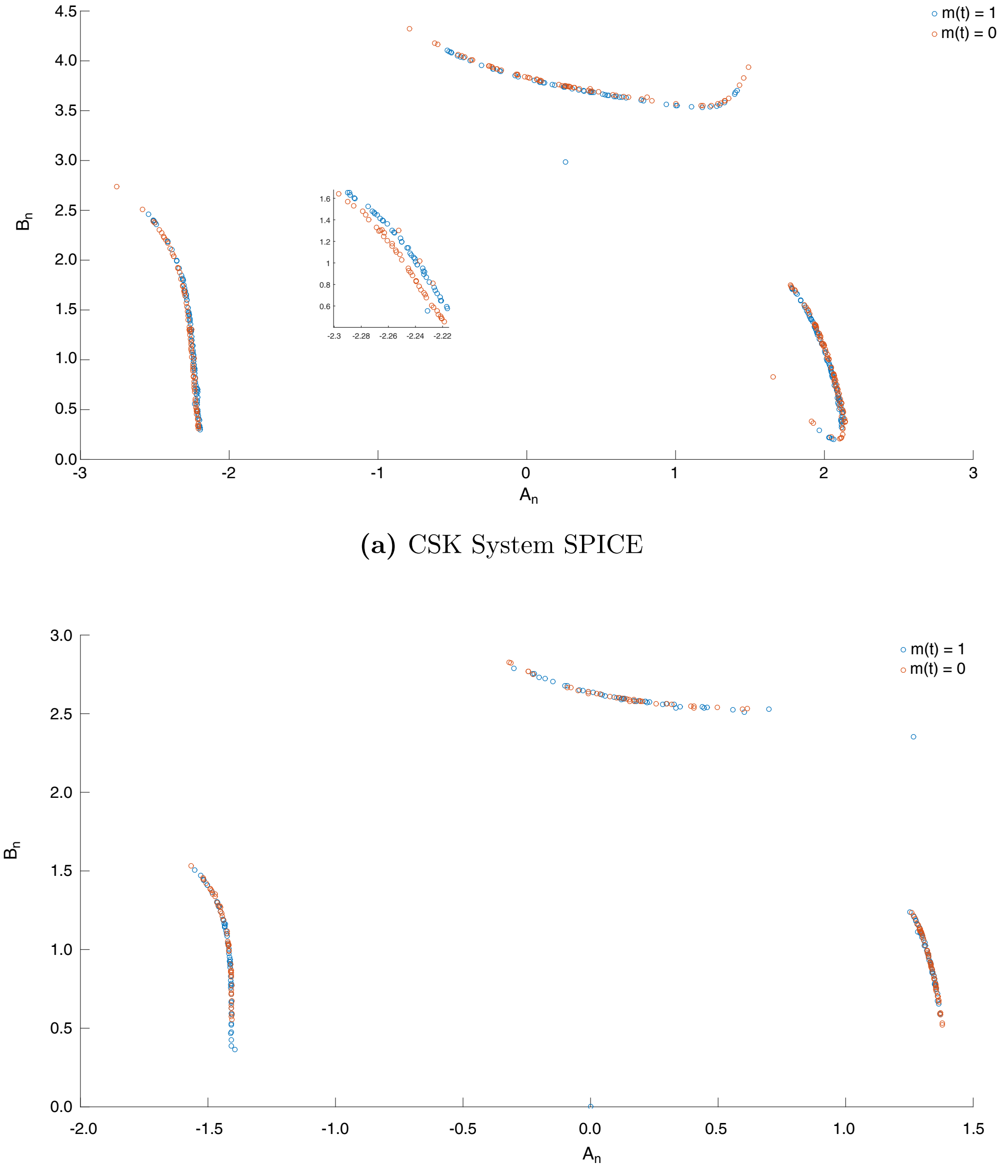
Figure 4.1: The sent signal $x_1(t)$ vs the message $m(t)$



(a) CSK System Simulink

(b) TS-CSK System Simulink

Figure 4.2: Return Maps from Simulink Simulation



(a) CSK System SPICE

(b) TS-CSK System SPICE

Figure 4.3: Return Maps from SPICE circuit simulations

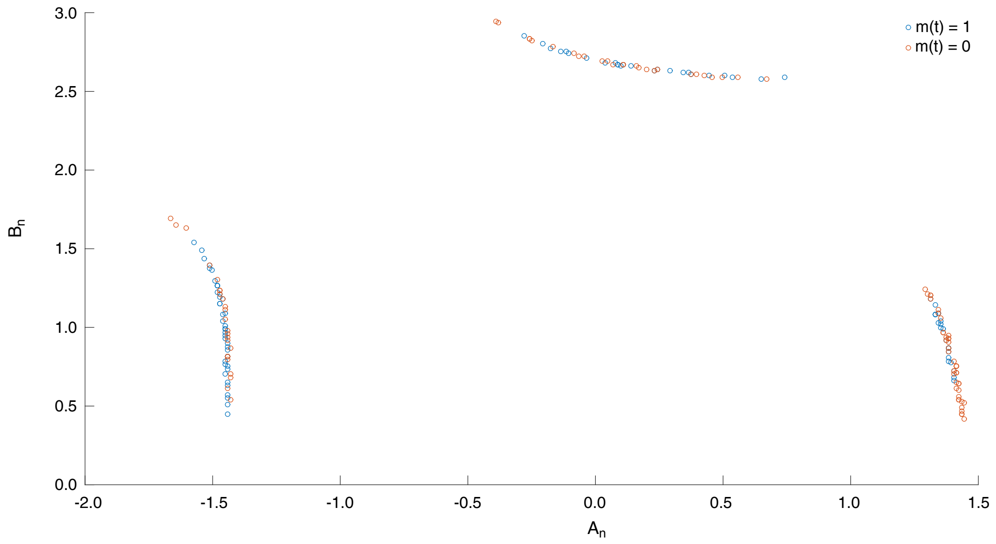
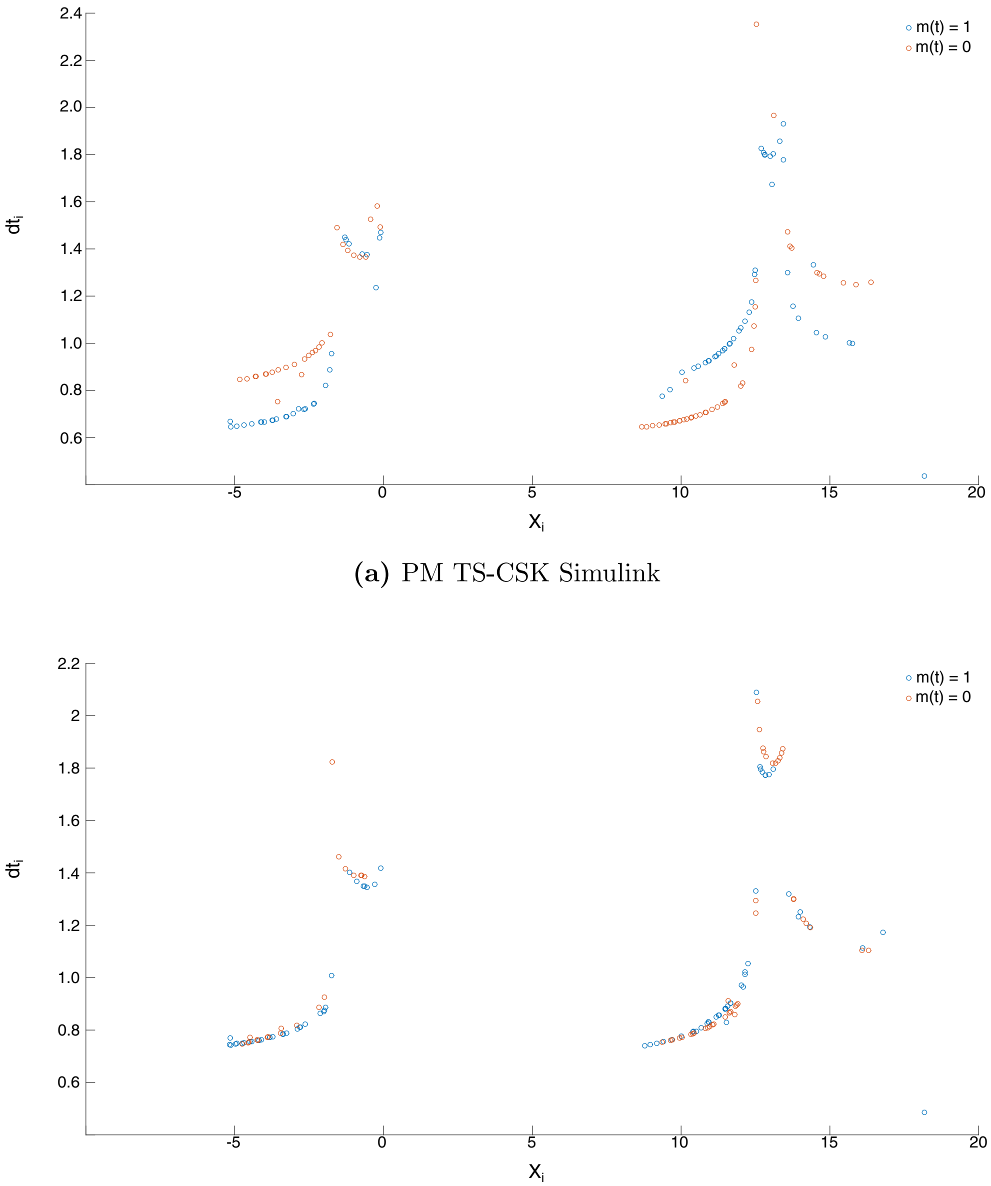


Figure 4.4: Return Map of TS-CSK system in circuitry

in numerical simulations for both the CSK and TS-CSK system, respectively. An exploded detail to show the difference in bit paths for the CSK system is seen in Figure 4.2a. Figure 4.3a and Figure 4.3b show the RMs derived from LTSPICE simulations. Figure 4.4 shows the RM gathered from the actual circuit. The TS-CSK system used to compare to the CSK system is the 8-section TS-CSK system, although the PM TS-CSK system demonstrates a similar RM. These RMs were measured using an alternating bit pattern at a frequency of 1 Hz for the circuit simulation and actual data, no bit padding is added to any bit.

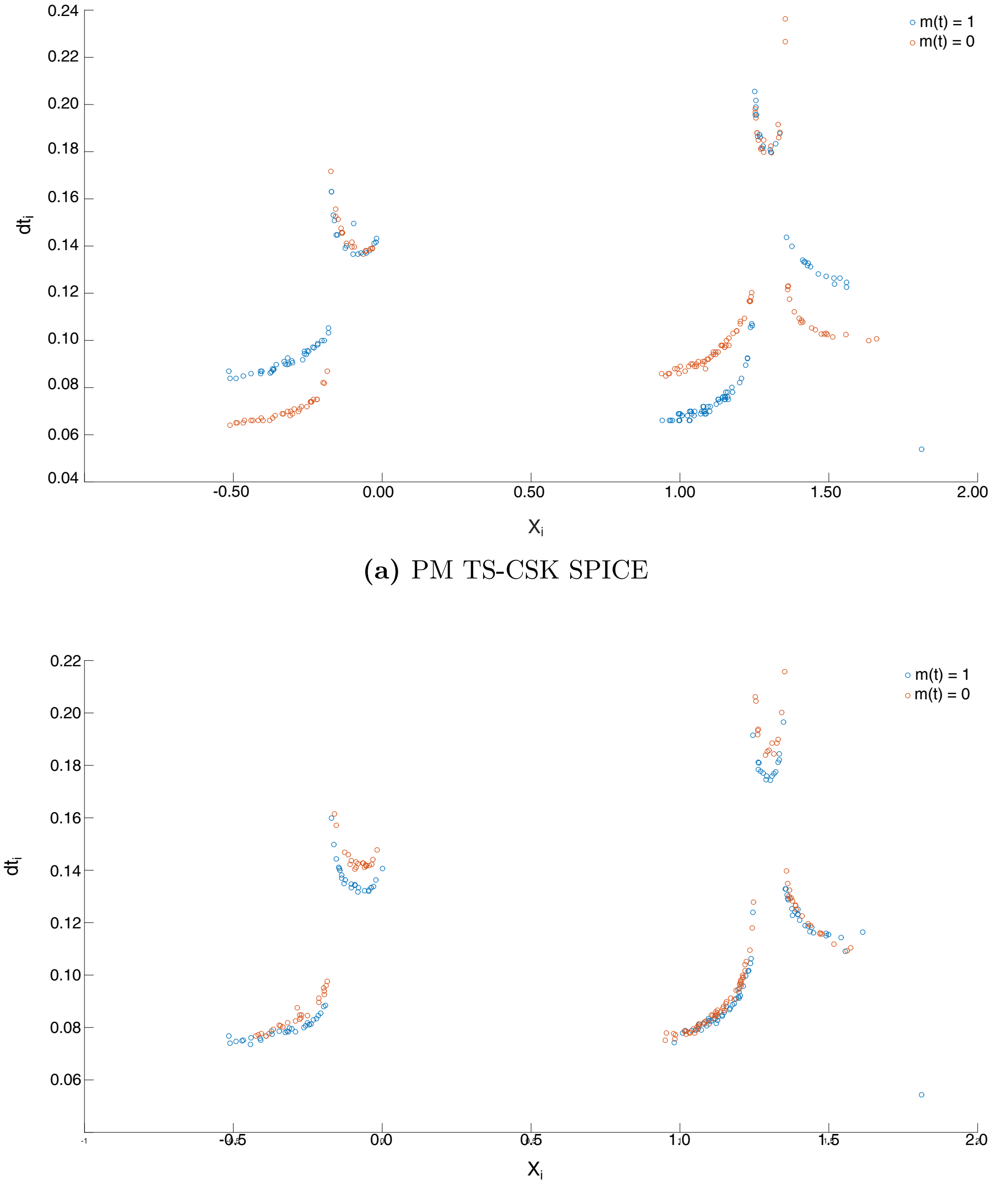
Figure 4.8 shows the bit error rate (BER) of the TS-CSK with added noise. The graph is scaled to show BER versus the signal to noise ratio of transmitted signal $x_1(t)$ in decibels (dB). The data was gathered using an arbitrary cutoff χ as described in Section 3.1.3. The weighting function $\phi(n)$ is selected with a weighting band $w = 0.8$ as described by (3.6). Figure 4.10 shows the LTSPICE simulation of the worst possible case parameter mismatch caused by component tolerance issues. This selection was chosen from a Monte-Carlo simulation consisting of 300 runs, where reference voltages were set at worst possible mismatch according to manufacturer



(a) PM TS-CSK Simulink

(b) 8-section TS-CSK Simulink

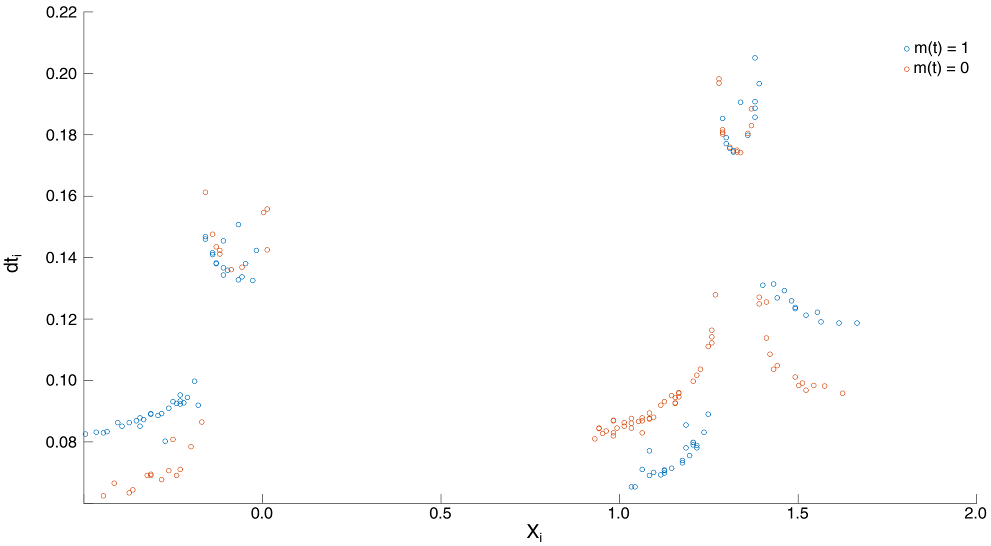
Figure 4.5: Return Time Maps from Simulink simulation



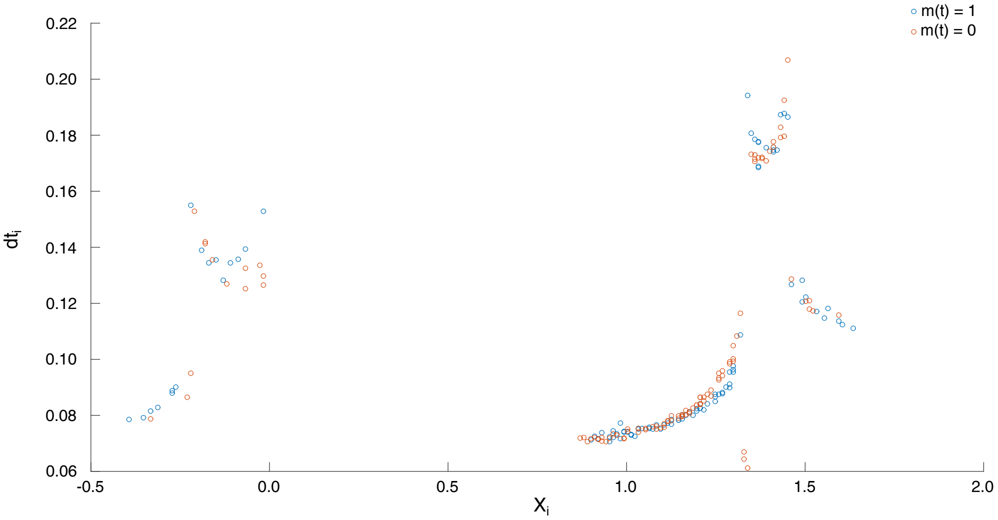
(a) PM TS-CSK SPICE

(b) 8-section TS-CSK SPICE

Figure 4.6: Return Time Maps from SPICE simulation



(a) PM TS-CSK Actual Circuit



(b) 8-section TS-CSK Actual Circuit

Figure 4.7: Return Time Maps from circuit implementations

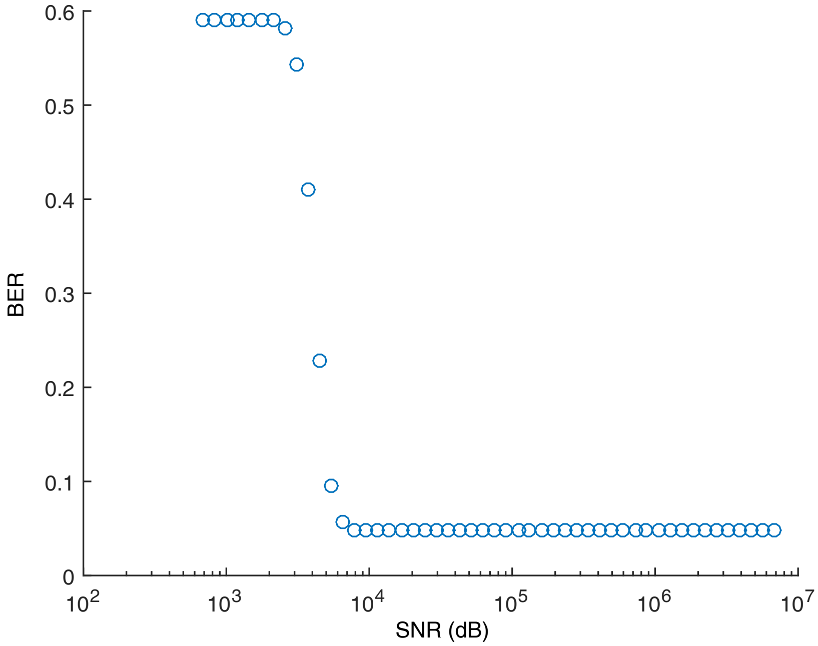
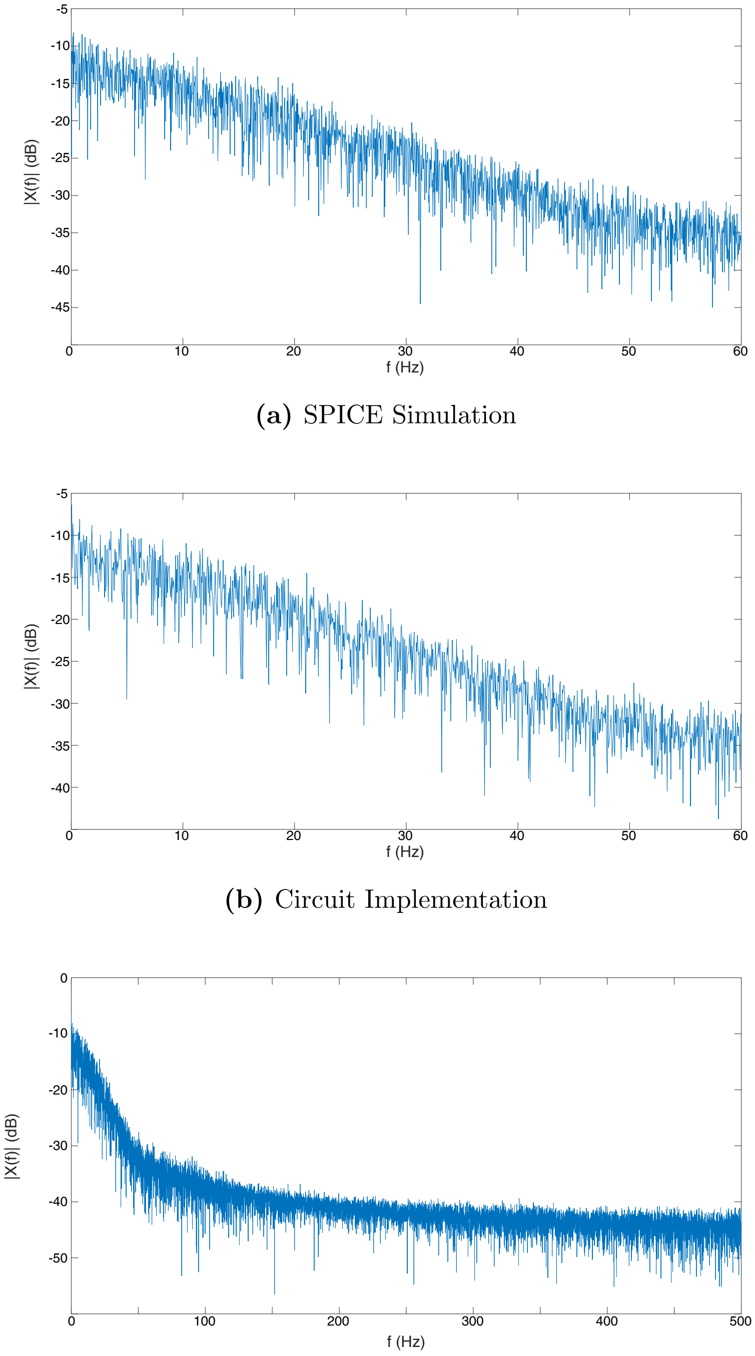


Figure 4.8: Noise and Parameter Mismatch Characteristics

tolerances. The top figure shows the error $\Phi_1(t) = x_1(t) - z_1(t)$, the center figure shows $\Phi_1^2(t) = \big(x_1(t) - z_1(t)\big)^2$ and the bottom figure shows $m(t)$.

Figure 4.9 shows the fast Fourier transform (FFT) of the transmitted signal $x_1(t)$ with a 0.5 Hz alternating bit signal. Figure 4.9a shows the simulation FFT in LTSPICE, while Figure 4.9b shows the FFT of the actual circuit. The SPICE simulation data set required interpolation to obtain a fixed time sample to perform the FFT. Figure 4.9c shows a wider power spectral density (PSD) view of the actual circuit.

Table 4.1 shows the results of a randomly selected plain-text message encryption test. A file of initially 2500 characters was randomly generated from ASCII characters in the range of HEX value 0x20 to 0x7E. The bound on these characters was due to communication issues via UART between MATLAB and the message signal generator for characters greater than 0x7E. The Simulation test required a larger file. 10000 additional randomly generated characters are appended onto the first 2500 for the Simulink simulation. The 8-section TS-CSK was limited to 1620 characters in the interest of time. The simulation obtained a BER of better than 10ppm at least,



(a) SPICE Simulation

(b) Circuit Implementation

(c) Wider PSD Circuit Implementation

Figure 4.9: Fast Fourier transform (FFT) of the 8-section TS-CSK system in circuitry

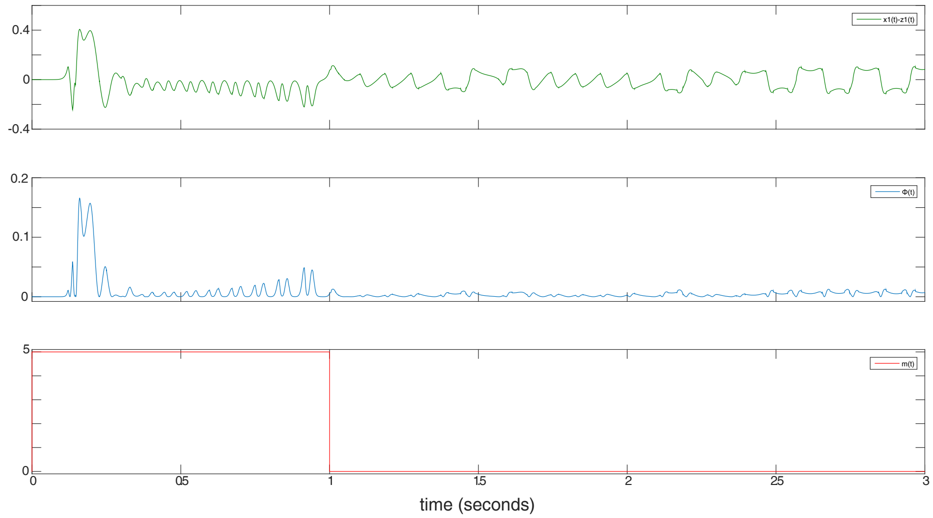


Figure 4.10: Noise and Parameter Mismatch Characteristics

while the PM TS-CSK and 8-section TS-CSK practical circuits obtained BERs of 800ppm and 3000ppm respectively. The practical tests did not sequentially encrypted characters due to limitations of the data acquisition equipment, the simulation did sequentially encrypted all 12500 characters. The practical experiment took approximately 6.5 hours and 12 hours to complete for the PM TS-CSK and 8-section TS-CSK respectively. The 8-section TS-CSK used a message frequency of 0.5 Hz while the PM TS-CSK used a message frequency of 1Hz. The 8-section TS-CSK circuit required a slower message frequency due to poor synchronization.

Table 4.1: Bit Error Rate (BER) Test Results

	Simulation	Practical (P&M)	Practical (8 State)
High Misses	0	0	38
High Bits	47964	9658	6234
Low Misses	0	16	0
Low Bits	52036	10342	6726
Total Misses	0	16	38
Total Bits	100000	20000	12960
Miss Rate	$< 1\text{x}10^{-5}$	$8\text{x}10^{-4}$	$3\text{x}10^{-3}$

Chapter 5

Conclusions

This thesis has detailed the process of creating the encryption system itself, and as such should be seen as a starting point for product potential. In this chapter the performance of the TS-CSK system as a whole will be evaluated, the potential performance improvements described, and the practical considerations for this system for use in real-life secure transmission systems.

5.1 System Performance

The performance of the 8 state TS-CSK system, with comparison to the CSK and PM TS-CSK system, shows the potential for this cryptographic method in practical implementation. The overall performance of the TS-CSK system can be broken into several sections. The most important performance characteristic to practicality is the synchronization performance, followed by the noise performance, the mismatch performance, and lastly the security performance. While security is paramount for any encryption system, functioning synchronization, noise and mismatch performance dictate the usability. If the security is weak, and the other performance good, the system can be used as a weak encryption method. In the instance the security is strong, but the real system fails to synchronize in practice, the system is of little use practically.

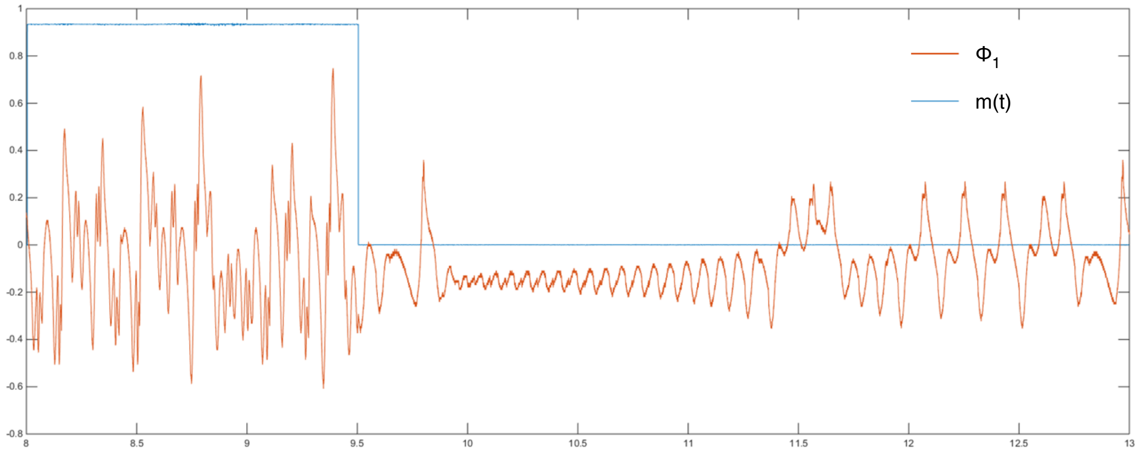


Figure 5.1: The Synchronization Error Φ vs the scaled message $m(t)$ of the 8 section TS-CSK circuit

5.1.1 Synchronization Performance

The synchronization performance of the TS-CSK system is evaluated in an overall manner by Table 4.1. The first column depicts the 8-state TS-CSK system simulated in MATLAB and Simulink. As can be seen after having processed 12500 characters, not a single bit error was made from the simple weighted averaging over bit periods described in Section 3.1.3. This performance shows a bit error rate (BER) performance of better than 10 parts per million (ppm).

The second column of Table 4.1 shows the BER gathered from a test of the simple PM TS-CSK system. As is shown the performance is decreased by at least an order of magnitude at 800 ppm BER. The last column shows the 8-state TS-CSK system with a performance of 3000 ppm BER, or otherwise stated as a 0.3% BER.

The performance of the PM TS-CSK system is acceptable, and if implemented with parity checking would not degrade communication quality or speed significantly. The 8-state TS-CSK system however has near quadruple the amount of errors of the PM TS-CSK system. Interestingly in both cases the optimum cutoff value lead to a strictly low miss for the PM TS-CSK system and a strictly high miss for the 8-section TS-CSK system.

In the instance of the PM TS-CSK it could be seen that at certain bit changes to 1 the magnitude of the synchronization error Φ was much smaller than that of other bit changes to 1. This lead to the asymmetric bit type miss rates for optimum BER. Figure 5.1 shows that in some cases the 8-state TS-CSK system suffered almost no magnitude change between 0 and 1 bits. This caused the 8-state TS-CSK system to also have bit changes to 1 that could not be extracted from the synchronized background. Notably Figure 5.1 also shows that during the non-synchronizing bit Φ has an increased frequency.

5.1.2 Noise Performance

The BER caused by noise of the TS-CSK system has a rather sharp cutoff for the simple weighted averaging method. Figure 4.8 shows the response of the TS-CSK system to input noise. As can be seen at a signal-to-noise ratio (SNR) of less than approximately 40dB leads to the a sudden rise from a near perfect BER to a complete loss of all 0 bits. Cisco Meraki recommends a SNR of 25dB for voice applications and 20dB for data networks in wireless communications. An improvement of performance to the TS-CSK system to decrease the minimum SNR would be necessary for use in standard wireless communication systems.

5.1.3 Mismatch Performance

Monte-Carlo simulations of the 8-section TS-CSK system in SPICE with resistor and capacitor tolerances. taken into account indicated that synchronization, with the selection of high accuracy components, should have been excellent. This was not what was observed in real circuitry, synchronization mismatch became quite severe within the 8-section TS-CSK system, as is seen in Figure 5.1. Figure 4.10 then shows the results later gathered with the maximum offsets applied to the reference voltages in a worst case scenario along with passive component tolerances. This result comes more in line with what was observed within actual circuitry.

The new Monte-Carlo simulations indicate that this synchronization error is not derived from the passive component mismatch, but rather from the mismatch of zener diode regulation voltage. Both the transmitter and receiver have a separate decision engine board, so while the origin crossing point will be the same for both the upper and lower foci and third state foci set point will inherently be different as the zener diodes chosen are limited to ±1% accuracy.

An additional source of synchronization mismatch of the live circuit could be attributed to the solderless breadboard performance. Two breadboards were used with the circuit. One was used to gather all results within this work. The second slightly larger breadboard failed to allow the circuit pair to function. The issue was noted, but further experimentation was not completed to discern the cause of failure of one breadboard over the other. The breadboard that failed has been used in other circuitry prototyping.Supply voltages were verified with a digital multimeter across both breadboards.

5.1.4 Security Performance

To evaluate the security of the TS-CSK encryption scheme and the vulnerabilities of a chaotic encryption scheme several comparisons and tests were performed. To ensure good system security the TS-CSK system's return and return time maps are compared for security, and the standard methods of cryptanalysis considered.

Return Map Attack Immunity

The return maps (RM) for both a standard CSK and a TS-CSK system were determined. These RMs are shown in Figures 4.2, 4.3, and 4.4 starting on page 42. The CSK system RM can be seen in Figure 4.2a as calculated from the MATLAB and Simulink model, another RM generated from the LTSPICE model can be seen in Figure 4.3a. Likewise Figures 4.2b and 4.3b show the RM for the TS-CSK system as calculated from the MATLAB and LTSPICE models respectively. Additionally the

RM of the constructed TS-CSK circuit can be seen in Figure 4.4.

The CSK RMs clearly show a distinction from the maximums that exist at $m(t) = 0$ and $m(t) = 1$ once a single region is selected and the scale expanded. This is due the small difference between β_0 and β_1. The distinction becomes more ambiguous towards the ends of each streak, however the majority of minimums and maximums measured show clear distinction. The effect of noise on the RM of a CSK system was not analyzed. Materassi and Basso argue that while noise would distort a RM it would also adversely effect system performance, and as such cannot be relied upon to defeat the RM.

The TS-CSK system with encryption of the message $m(t)$ encoded within a time scaling factor is easily shown to be immune to the RM as was expected by Section 2.3.1. The RM shown in Figure 4.4 was obtained using a noisy power supply and a simple DAQ device, the RM shows a very similar structure to that calculated from both simulation types. It was noticed that the extraction of the local minimums and maximums was more complicated than that of the simulated systems, as line noise and DAQ resolution had to be taken into account. The almost linear distribution of points from Figure 4.4 is due to poor DAQ resolution.

Return Time Map Attack Immunity

The return time map (RTM) attack simulations can be seen in Figures 4.5, 4.6 and 4.7 starting on page 45. The figures show the simple PM TS-CSK system in comparison to the 8 section TS-CSK system. Figures 4.5a and 4.5b show the RTMs from the MATLAB simulation of the PM TS-CSK and 8 section TS-CSK systems respectively. Figures 4.6a and 4.6b show the RTMs from the SPICE simulation of the PM TS-CSK and 8 section TS-CSK systems respectively. Lastly Figures 4.7a and 4.7b show the RTMs calculated from live gathered data for the PM TS-CSK and 8 section TS-CSK systems respectively.

It is clear to see from the RTMs that the PM TS-CSK method is wholly vulnerable to the RTM attack. Even in data gathered from the real world circuit with low-end

DAQ equipment, the distinction between $m = 1$ and $m = 0$ states is significant. The effectiveness of this method with low cost equipment indicates that unlike parameter estimation from live measurement, this RTM attack does not require precise or expensive equipment to perform and be successful.

The 8 section TS-CSK method does show some splitting between modes in the positive orbit to negative orbit changed, shown by the upper left set formed. This was observed strongly in the SPICE simulation, however not as strongly in the MATLAB simulation and with even greater ambiguity in the real world acquisition. This is also seen for the negative orbit to positive orbit change to a lesser degree from the upper right set. The orbits about the positive and negative foci are shown to be completely immune.

Ciphertext attacks

Menezes et al. lists a series of attacks that are typically applied to digital encryption methods and ciphers. While not all of the methods listed by Menezes et al. apply to the chaotic analog encryption scheme of the TS-CSK system, some do warrant short investigation.

Ciphertext-Only Attack

The RM and RTM are ciphertext-only attacks. Vulnerability to this attack leaves the encryption method entirely insecure (Menezes et al., 1996). The PM TS-CSK and CSK systems are then easily proven to be completely insecure by the RTM and RM attacks respectively. Outside of the RM or RTM approach, the only other method of attack that can be made from ciphertext-only would be an attempt to estimate the foci points from the transmitted state. This method has been shown to break the security of the CSK system as well (Orue et al., 2006).

The estimation of the foci however only provides a ratio function to the adversary (Orue et al., 2006). As the only foci that can be estimated from the two possible transmission states of the Lorenz system are the $x_1(t)$ and $x_2(t)$ states. Therefore the only relation that can be drawn from the estimated foci, x_C, is:

$$x_C = \pm\sqrt{\rho(\beta - 1)}$$

This relation is very useful if either the ρ or β parameter is changing, however the TS-CSK system doesn't exhibit this. This relation only serves to reduce the potential key-space possibilities, which for a TS-CSK system is countered by the ability to have the $\lambda(x, m)$ term be a portion of the key space.

Known-Plaintext and Chosen-Plaintext Attacks

The form of attack derived from inserting a known plain-text message and then drawing comparisons to the responding "ciphertext" is not applicable to any CSK system implemented in circuitry. The message will only effect the orbitals or orbital speed regime for CSK and TS-CSK system receptively. A repetition of ciphertext will only apply when the initial conditions of the system can be guaranteed, which is not possible within a circuit without internal knowledge of the Lorenz system and significantly accurate measurements of the state values.

Sweeping Parameters

The brute force method of breaking the CSK or TS-CSK encryption involves an adversary designing a receiver with the same topology and with a sample of ciphertext sweeping parameters until synchronization is achieved for one instance. As with the RM and RTM attack, once a synchronizing configuration is found the adversary can retrieve the underlying bit change structure and decrypt two separate possibilities. This method is only practical to apply in the instance that the key space is small enough and an accurately reproducible sample is available.

Key Space

Other than defeating a RM attack, the TS-CSK also provides a much greater key space. If the switching events are obfuscated sufficiently to remove vulnerability to the RTM attack, the parameters λ_0 and λ_1 can be used to greatly increase the keyspace of the provided underlying Lorenz system.

The size of the keyspace can be described as:

$$\begin{aligned}
k_L &= \text{The available keyspace of the Lorenz system} \\
k_S &= \text{The available keyspace of the Time Scaling system} \\
k_T &= \text{The number of decision engines immune to TS and TS-CSK} \\
k_{FULL} &= k_L k_S k_T
\end{aligned}$$

k_L will have a corresponding range for each key about which it will still synchronize well enough to perform bit extraction. As such k_L will be finite due to the synchronization band limit and the limitation of parameter combinations capable of providing a chaotic system that will operate within a region of circuitry that is sufficient. The parameter ranges and bounding are described in Section 2.1.

k_S has limitation imposed by general circuitry speed response concerns, as well as power spectral density (PSD) spread concerns. k_T is limited by the methods that lead to RTM immunity and that provide a practical method for implementation.

5.2 Practical Considerations

The TS-CSK system created for this work has shown considerable promise for use within a commercial communication system. However, the current method of bit extraction, minimum SNR, and other synchronization error issues prevent this exact method from having practical use with a communication system without improvements and modifications.

5.2.1 Synchronization Improvement

Improvements to synchronization within the real circuit would significantly increase the practical usage capability of the TS-CSK as a real-world encryption device. Improvement opportunities exist in the circuitry, bit extraction method, and switching decision methods.

Circuitry Improvements

There are several improvements to the electrical circuit of the TS-CSK system that could be made in future work. The largest issue seen in synchronization mismatch seemed to be derived from unequal reference voltages in the decision engines. A higher accuracy voltage source along with a tuned reference would likely provide greater precision between mirrored switching reference points. Likewise, a controlled tuning reference could also take into account voltage differences that may occur in real applications due to local ambient differences.

Circuit noise improvements would also be available. While the majority of the circuitry and components are retained onto either the dynamics PCB or the decision engine PCB, which both have ground planes, inter-board connections still use the breadboard interface. A purpose-built PCB could be developed to contain sockets for the dynamics and decision PCBs as well as power and measurement connections. The power supply itself, a personal ATX power supply claims to be low noise and ripple, however no datasheet is available for the power supply used. The use of a higher quality power supply could also reduce noise.

Bit Extraction

The simple weighted periodic averaging method used for bit extraction in this work is highly susceptible to noise and mismatch in synchronization. Bit extraction becomes increasingly difficult as the difference between synchronous and non-synchronous bits shrinks. A peak detection method may work more adequately, where the peaks of Φ

above some threshold within an integration section are averaged and a running tally is used to provide an additional weighting factor. This method might be adequate to extract bits from synchronization signals like that of Figure 5.1.

Other methods of bit extraction could be created around some other pattern recognition algorithm. However, for one of the intended uses of this work. Extraction algorithms that require heavy software processing are not desired. The error present from synchronization mismatch rather than a non-synchronous bit should also be explored in future work. A difference in power spectral density between error causes could potentially lead to a filtering option to improve simple bit extraction methods.

Switching Decision Methods

The switching decision chosen to limit the need for high speed ADC devices is shown in this work to function, but at a far worse BER than the more simple yet insecure two state PM TS-CKS switching decision. Improvements to this method could possibly be obtained by performing a linear adjustment function set to one or more states and then comparing to the ground reference, i.e. the origin. Two decisions which would not rely on an external voltage reference and would provide a 4 region switching plain:

$$a_0 = \begin{cases} 0 & x_2 \geq x_1 \\ 1 & x_2 < x_1 \end{cases}$$
$$a_1 = \begin{cases} 0 & x_2 \geq 0 \\ 1 & x_2 < 0 \end{cases} \tag{5.1}$$

$$\delta(x) = (a_0 \oplus a_1) \oplus m(t) \tag{5.2}$$

(5.1) and (5.2) could further be expanded in some manner by also comparing the x_2 or x_1 with x_3 to double the regions generated. Again these regions would also not rely on an external source.

5.2.2 Wireless Transmission Usage

Figure 4.9 shows the LTSPICE simulation and live gathered FFT of the TS-CSK system. As can be seen the system implemented in this work has a narrow band. Figure 4.8 shows that any CSK method is not fit for use with amplitude modulation (AM) methods and wireless transmission use will require phase or frequency modulation (PM/FM) or other noise robust methods. Future work to implement the TS-CSK system in a standard FM band for personal communications, especially those used by police and military forces, is the next step in bringing the TS-CSK system to full utility.

5.3 Closing Remarks

The TS-CSK system promises to secure a near 30 year old method of analog encryption proposed by Pecora and Carroll. Further more an initial mistake made by the author of this thesis allowed for live circuit bit extraction using an RTM attack for the PM TS-CSK system, showing the effectiveness of this method with low-end equipment and real-world noise concerns. A second method of switching decision was conceived in haste that defeated the RTM that did not rely on an analog to digital converter (ADC), the 8-section TS-CSK system.

This work has shown that while the simulation results show good synchronization of the 8-section TS-CSK system, the actual circuits dependency on voltage references for the decision engine do not provide adequate results. It should considered from this result that an ADC switching scheme will rely on a likewise mismatched voltage source pair. A greater method of robust synchronization in the decision engine will greatly improve this system's field use as an encryption system. Further work should investigate FM broadcast capability in both analog form and a DSP processed digital form. Additionally by reducing the value of the capacitor that forms the op amp integrator to increase the speed gain k should be completed in future work to bring allowable communication rates to practical speeds.

Bibliography

Analog Devices (2015). AD633. http://www.analog.com/media/en/technical-documentation/data-sheets/AD633.pdf. 79

Candaten, M. and Rinaldi, S. (2000). Peak-to-peak dynamics: A critical survey. *International Journal of Bifurcation and Chaos*, 10(08):1805–1819. 16

Cisco Meraki (2015). Wireless fundamentals:Signal-to-Noise Ration (SNR) and wireless signal strength. https://documentation.meraki.com [Accessed: 03/2017]. 53

Cuomo, K. M. and Oppenheim, A. V. (1993). Circuit implementation of synchronized chaos with applications to communications. *Physical review letters*, 71(1):65. 10, 12, 14

Daemen, J. and Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media. 2

DeCarlo, R. A. and Lin, P.-M. (1994). *Linear circuit analysis (vol. 1): a time domain and phasor approach*. Prentice-Hall, Inc. 22

Dedieu, H., Kennedy, M. P., and Hasler, M. (1993). Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuits. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 40(10):634–642. 10

Horowitz, P. (2016). The Horowitz Group. http://seti.harvard.edu/ [Accessed: 10/2016]. 31

Horowitz, P. and Hill, W. (1983). *The art of electronics*. Cambridge University Press Cambridge. 21

Irving, R. S. (2003). *Integers, polynomials, and rings: a course in algebra*. Springer Science & Business Media. 8

Keen, J. (2003). *Harold'Doc'Keen and the Bletchley Park bombe/by John Keen*. M & M Baldwin. 2

Liu, J.-M. and Tsimring, L. S. (2006). *Digital communications using chaos and nonlinear dynamics*. Springer Science & Business Media. 2

Lorenz, E. N. (1963). Deterministic nonperiodic flow. *Journal of the atmospheric sciences*, 20(2):130–141. 3, 14

Lu, J., Wu, X., and Lü, J. (2002). Synchronization of a unified chaotic system and the application in secure communication. *Physics Letters A*, 305(6):365–370. 2

Makris, G. and Antoniou, I. (2012). Cryptography with chaos. In *5th Chaotic modelling and simulation international conference*, pages 12–15. 2

Materassi, D. and Basso, M. (2008). Time scaling of chaotic systems: Application to secure communications. *International Journal of Bifurcation and Chaos*, 18(02):567–575. 18, 19, 55

Maxim-Integrated (2017). Analog switches and multiplexers macromodels. https://www.maximintegrated.com/en/design/tools/modeling-simulation/spice/analog-switches-and-multiplexers/macro/. 36

Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press. 56

Oppenheim, A. V., Wornell, G. W., Isabelle, S. H., and Cuomo, K. M. (1992). Signal processing in the context of chaotic signals. In *Acoustics, Speech, and Signal Processing, 1992. ICASSP-92., 1992 IEEE International Conference on*, volume 4, pages 117–120. IEEE. 10

Orue, A., Alvarez, G., Romera, M., Pastor, G., Montoya, F., and Li, S. (2006). Lorenz system parameter determination and application to break the security of two-channel chaotic cryptosystems. *arXiv preprint nlin/0606029*. 56

Pecora, L. M. and Carroll, T. L. (1990). Synchronization in chaotic systems. *Physical review letters*, 64(8):821. 10, 61

Pérez, G. and Cerdeira, H. A. (1995). Extracting messages masked by chaos. *Physical Review Letters*, 74(11):1970. 14

Pincock, S. (2006). *Codebreaker: The History of Codes and Ciphers*. Walker & Company. 1

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126. 2

Sampei, M. and Furuta, K. (1986). On time scaling for nonlinear systems: Application to linearization. *IEEE Transactions on Automatic Control*, 31(5):459–462. 17

Sebag-Montefiore, H. (2011). *Enigma: the battle for the code*. Hachette UK. 1

Slotine, J.-J. E., Li, W., et al. (1991). *Applied nonlinear control*, volume 199. prentice-Hall Englewood Cliffs, NJ. 9

Sparrow, C. (2012). *The Lorenz equations: bifurcations, chaos, and strange attractors*, volume 41. Springer Science & Business Media. 3, 6, 7, 8

Swinnerton-Dyer, P. (2001). Bounds for trajectories of the lorenz equations: an illustration of how to choose liapunov functions. *Physics Letters A*, 281(2):161–167. 9, 10, 14

Texas Instruments (2004). *AN-31: Op Amp Circuit Collection*. Texas Instruments. Rev. 05/2013. 22

Thompson, J. E. (2016). Analog innovations. http://www.analog-innovations.com. Accessed: 2016-08-02. 36

Yang, T., Yang, L.-B., and Yang, C.-M. (1998). Cryptanalyzing chaotic secure communications using return maps. *Physics Letters A*, 245(6):495–510. 16

Appendix

Appendix A

Decision Engine Circuit

Figure A.1 shows the circuit for the decision engine as described by (2.36). The components used to construct the decision engine are listed in Table A.1. Figure A.2 shows the decision engine circuit for the PM TS-CSK system.

Table A.1: Component Values of the λ-Modulator Circuit

Index	Value	Manufacturer	Part Number
R_1, R_4, R_{19}	$100\,\text{k}\Omega$	Yageo	RT0603BRD07100KL
R_2, R_5	$261\,\text{k}\Omega$	Panasonic	ERA-3AEB2613V
R_3, R_6	$102\,\text{k}\Omega$	Panasonic	ERA-3AEB1023V
$R_7, R_{10}, R_{13}, R_{16}$	$20\,\text{k}\Omega$	Yageo	RT0603BRD0720KL
$R_8, R_{11}, R_{14}, R_{17}$	$1\,\text{M}\Omega$	Stackpole	RNCF0603BKC1M00
$R_9, R_{12}, R_{15}, R_{18}$	$10\,\text{k}\Omega$	Yageo	RT0603BRD0710KL
D	1N4148	Micro Com.	1N4148WX-TP
C	$3\,\text{nF}$	Murata	GRM1885C1H302JA01D
Z	-	Texas Inst.	LT1004IPWR-2-5
U_1, U_2, U_3, U_4	-	Linear Tech.	LT1011CS8#PBF
U_5	-	ON Semi.	MC74HC00ADR2G
U_6	-	Texas Inst.	SN74HC266DR

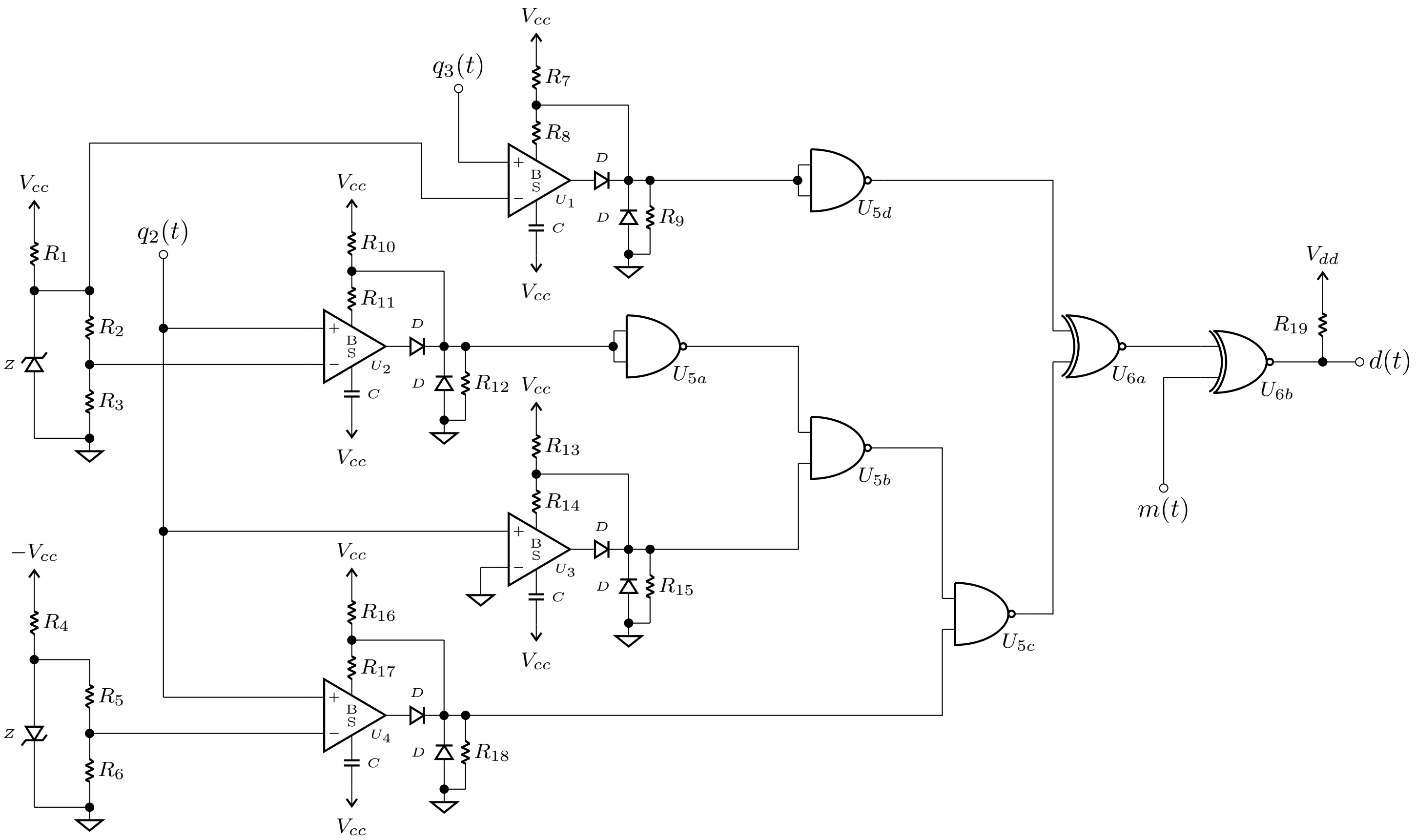


Figure A.1: 8 Section TS-CSK Decision Block Circuit

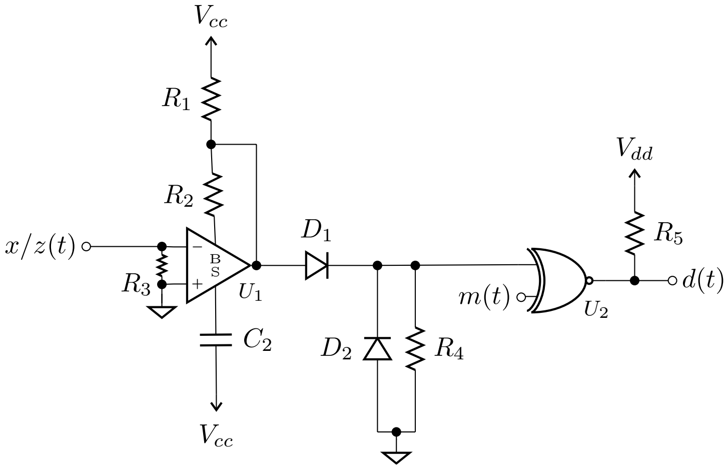


Figure A.2: PM TS-CSK Decision Block Circuit

Appendix B

Component Listing

B.1 Listing of Components Used in Circuit from Figure [3.11]

The following pages contain the component listing for all components used within the main dynamics PCBs.

Board Index	Value	Figure	Figure Index	Manufacturer	Part Number	Footprint
R_1	100 kΩ	3.7	R_1	Yageo	RT1206BRD07100KL	R1206
R_2	100 kΩ	3.7	R_2	Yageo	RT1206BRD07100KL	R1206
R_3	39 kΩ	3.7	R_4	Panasonic	ERA-8AEB393V	R1206
R_4	10 kΩ	3.7	R_5	Yageo	RT1206BRD0710KL	R1206
R_5	1 MΩ	3.7	R_3	Yageo	RT1206BRD071ML	R1206
R_6	10 kΩ	3.7	R_7	Yageo	RT1206BRD0710KL	R1206
R_7	499 kΩ	3.7	R_6	Yageo	RT1206BRD07499KL	R1206
R_8	100 kΩ	3.8:X	R_1	Yageo	RT1206BRD07100KL	R1206
R_9	100 kΩ	3.8:X	R_2	Yageo	RT1206BRD07100KL	R1206
R_{10}	100 kΩ	3.8:X	R_3	Yageo	RT1206BRD07100KL	R1206
R_{11}	15 kΩ	3.8:X	R_4	Stackpole	RNCF1206BKC15K0	R1206
R_{12}	100 kΩ	3.8:X	R_5	Yageo	RT1206BRD07100KL	R1206
R_{13}	76.8 kΩ	3.8:X	R_6	Panasonic	ERA-8AEB7682V	R1206
R_{14}	Short	-	-	-	-	R1206
R_{15}	Short	-	-	-	-	R1206
R_{16}	20 kΩ	A.1	R_1	Yageo	RT1206BRD0720KL	R1206
R_{17}	1 MΩ	A.1	R_2	Yageo	RT1206BRD071ML	R1206
R_{18}	100 kΩ	A.1	R_3	Yageo	RT1206BRD07100KL	R1206

Board Index	Value	Figure	Figure Index	Manufacturer	Part Number	Footprint
R_{19}	100 kΩ	3.8:Y	R_1	Yageo	RT1206BRD07100KL	R1206
R_{20}	100 kΩ	3.8:Y	R_2	Yageo	RT1206BRD07100KL	R1206
R_{21}	100 kΩ	3.8:Y	R_3	Yageo	RT1206BRD07100KL	R1206
R_{22}	15 kΩ	3.8:Y	R_4	Stackpole	RNCF1206BKC15K0	R1206
R_{23}	100 kΩ	3.8:Y	R_5	Yageo	RT1206BRD07100KL	R1206
R_{24}	76.8 kΩ	3.8:Y	R_6	Panasonic	ERA-8AEB7682V	R1206
R_{25}	100 kΩ	3.8:Z	R_1	Yageo	RT1206BRD07100KL	R1206
R_{26}	100 kΩ	3.8:Z	R_2	Yageo	RT1206BRD07100KL	R1206
R_{27}	100 kΩ	3.8:Z	R_3	Yageo	RT1206BRD07100KL	R1206
R_{28}	15 kΩ	3.8:Z	R_4	Stackpole	RNCF1206BKC15K0	R1206
R_{29}	100 kΩ	3.8:Z	R_5	Yageo	RT1206BRD07100KL	R1206
R_{30}	76.8 kΩ	3.8:Z	R_6	Panasonic	ERA-8AEB7682V	R1206
R_{31}	10 kΩ	A.1	R_4	Yageo	RT1206BRD0710KL	R1206
R_{32}	100 kΩ	3.8:S	R_1	Yageo	RT1206BRD07100KL	R1206
R_{33}	100 kΩ	3.8:S	R_2	Yageo	RT1206BRD07100KL	R1206
R_{34}	100 kΩ	3.8:S	R_3	Yageo	RT1206BRD07100KL	R1206
R_{35}	15 kΩ	3.8:S	R_4	Stackpole	RNCF1206BKC15K0	R1206
R_{36}	100 kΩ	3.8:S	R_5	Yageo	RT1206BRD07100KL	R1206
R_{37}	76.8 kΩ	3.8:S	R_6	Panasonic	ERA-8AEB7682V	R1206

Board Index	Value	Figure	Figure Index	Manufacturer	Part Number	Footprint
C_1	0.1 µF	3.7	C	KEMET	C1812C104F5GAC7800	C1812
C_2	0.1 µF	3.7	C	KEMET	C1812C104F5GAC7800	C1812
C_3	0.1 µF	3.7	C	KEMET	C1812C104F5GAC7800	C1812
C_4	3 nF	A.1	C_2	Murata Elec. NA	GRM1885C1H302JA01D	C0603
C_5	short	-	-	-	-	C0603
D_1	-	A.1	D_1	Micro Com. Co.	1N4148W-TP	SOD-123
D_2	-	A.1	D_2	Micro Com. Co.	1N4148W-TP	SOD-123
IC_1	-	3.7	U_1, U_2	Linear Tech.	LT1057S8#PBF	8-SO
IC_2	-	3.8:X	U_1, U_2	Linear Tech.	LT1057S8#PBF	8-SO
IC_3	-	3.7	U_3	Linear Tech.	LT1057S8#PBF	8-SO
IC_4	-	3.8:Y	U_1, U_2	Linear Tech.	LT1057S8#PBF	8-SO
IC_5	-	3.8:Y	U_3	Maxim Int.	DG419LEUA+	8-μMAX
IC_6	-	3.8:Z	U_1, U_2	Linear Tech.	LT1057S8#PBF	8-SO
IC_7	-	3.8:X	U_3	Maxim Int.	DG419LEUA+	8-μMAX
IC_8	-	3.8:Z	U_3	Maxim Int.	DG419LEUA+	8-μMAX
IC_9	-	3.8:S	U_1, U_2	Linear Tech.	LT1057S8#PBF	8-SO
IC_{10}	-	3.8:S	U_3	Maxim Int.	DG419LEUA+	8-μMAX
IC_{11}	-	A.1	U_2	Texas Inst.	SN74HC266DR	14-SO
$U\$_1$	-	A.1	U_1	Linear Tech.	LT1011CS8#PBF	8-SO

Board Index	Value	Figure	Figure Index	Manufacturer	Part Number	Footprint
$U\$_2$	-	3.7	U_4	Analog Dev. Inc.	AD633ARZ-R7	8-SO
$U\$_3$	-	3.7	U_5	Analog Dev. Inc.	AD633ARZ-R7	8-SO
SV_1	-	-	-	Amphenol	68021-210HLF	0.1" Pitch
SV_2	-	-	-	Amphenol	68021-210HLF	0.1" Pitch
J_1	-	-	-	Sullins	PRPC040SFAN-RC	0.1" Pitch

Appendix C

Circuit Calculations

C.1 λ gain calculations

Ideal operational amplifier behavior is assumed, as such voltage and both inputs is equal, and neither inputs allow current in or out. Calculation variables are in reference to those depicted in figure [C.1]

$$
\begin{aligned}
v_m &= \left(\frac{R_1}{R_1 + R_2}\right)s \\
i_1 &= \frac{s}{R_3} \\
i_2 &= \frac{v_m}{R_5}
\end{aligned}
$$

For the top gain circuit

$$
\begin{aligned}
\frac{s}{R_3} &= \frac{v_1 - s}{R_4} \\
\frac{v_1}{R_4} &= \frac{s}{R_3} + \frac{s}{R_4} \\
v_1 &= \frac{R_4(R_3 + R_4)s}{R_3 R_4} \\
&= \left(1 + \frac{R_4}{R_3}\right)s
\end{aligned}
$$

For the bottom gain circuit

$$\begin{aligned}
\frac{v_m}{R_5} &= \frac{v_2 - v_m}{R_6} \\
\frac{v_2}{R_6} &= \frac{v_m}{R_5} + \frac{v_m}{R_6} \\
v_2 &= \frac{R_6(R_6 + R_5)v_m}{R_6 R_5} \\
&= \Big(1 + \frac{R_6}{R_5}\Big)v_m \\
&= \Big(1 + \frac{R_6}{R_5}\Big)\Big(\frac{R_1}{R_1 + R_2}\Big)s \\
&= \Big(\frac{R_1 R_5 + R_1 R_6}{R_1 R_5 + R_2 R_5}\Big)s
\end{aligned}$$

As such the impulse response of the λ gain can be expressed as:

$$\lambda(x/z, m)s(t) = \begin{cases} \Big(1 + \frac{R_4}{R_3}\Big)s & d = 0 \\ \Big(\frac{R_1 R_5 + R_1 R_6}{R_1 R_5 + R_2 R_5}\Big)s & d = 1 \end{cases}$$

Where d is determined as described in section [2.4] based on decision engine selection.

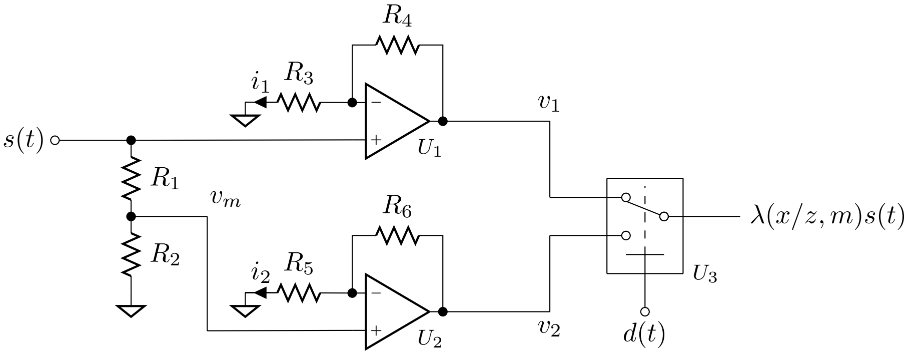


Figure C.1: λ Gain Circuit

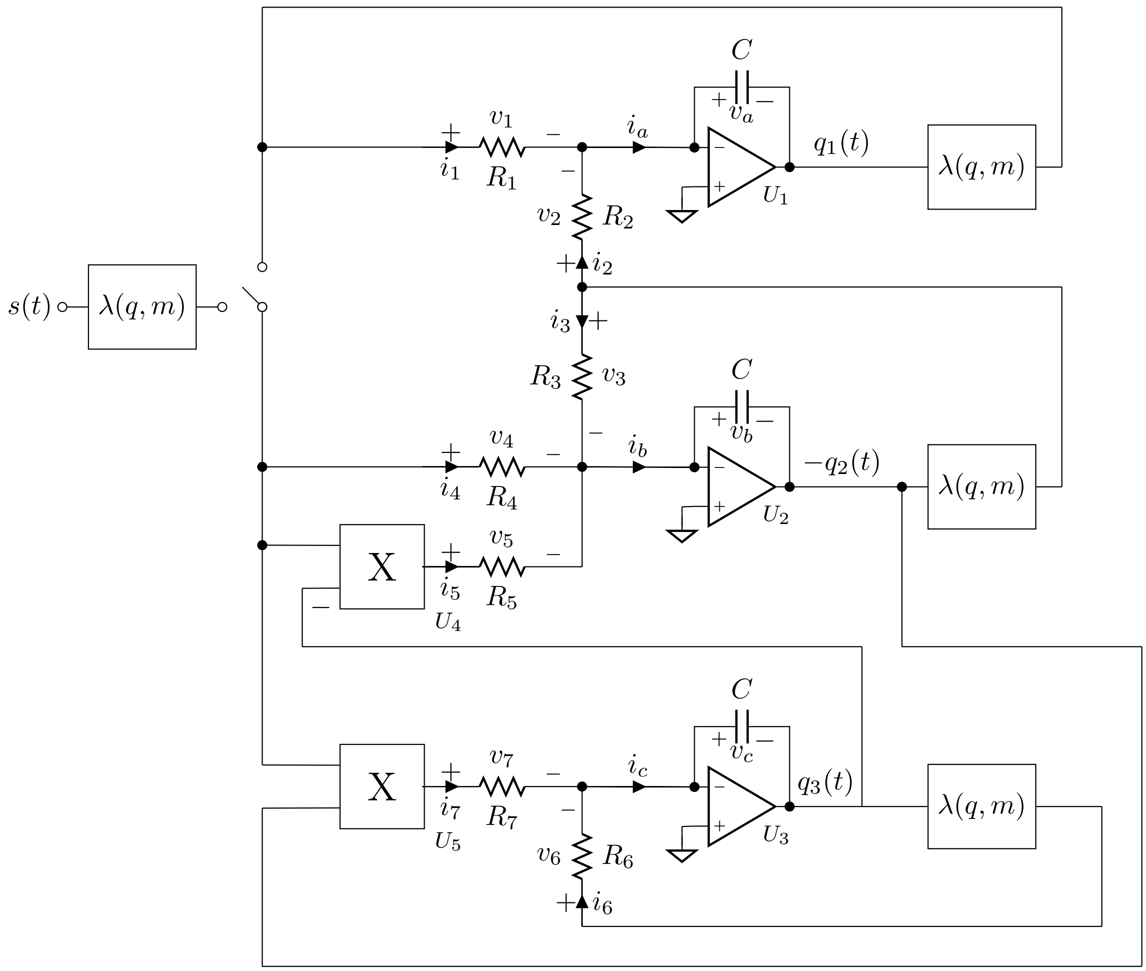


Figure C.2: TS-CSK Circuit

C.2 Full Circuit Calculations

Ideal operational amplifier behavior is assumed same as section [C.1]. The behavior of the multiplication blocks is as detailed from the AD633 datasheet (Analog Devices, 2015) as:

$$v_{out} = \frac{v_a v_b}{10\text{V}} + v_c$$

The multipliers are configured such that $v_c = 0$, and U_4 is configured such that the input v_b is inverted. The currents of the system with the switch set to select $\lambda q_1(t)$

are:

$$\begin{aligned}
i_a &= i_1 + i_2 \\
i_b &= i_3 + i_4 + i_5 \\
i_c &= i_7 + i_6 \\
i_1 &= \frac{\lambda q_1}{R_1} \\
i_2 &= -\frac{\lambda q_2}{R_2} \\
i_3 &= -\frac{\lambda q_2}{R_3} \\
i_4 &= \frac{\lambda q_1}{R_4} \\
i_5 &= \frac{(\lambda q_1)(-q_3)}{10\mathrm{V} R_5} \\
i_6 &= \frac{\lambda q_3}{R_6} \\
i_7 &= \frac{(\lambda q_1)(-q_2)}{10\mathrm{V} R_7}
\end{aligned}$$

The dynamics set by v_a:

$$\begin{aligned}
v_a &= \int \frac{i_a}{C}\ \mathrm{dt} \\
q_1 &= -v_a \\
&= -\int \frac{i_a}{C}\ \mathrm{dt} \\
\dot{q}_1 &= -\frac{i_a}{C} \\
&= -\frac{1}{C}\Big(\frac{\lambda q_1}{R_1} - \frac{\lambda q_2}{R_2}\Big)
\end{aligned}$$

Let $R_1 = R_2 = R$

$$\begin{aligned} &= -\frac{\lambda}{RC}(q_1 - q_2) \\ \dot{q}_1 &= \frac{\lambda}{RC}(q_2 - q_1) \end{aligned}$$

The dynamics set by v_b:

$$\begin{aligned} v_b &= \int \frac{i_b}{C}\ \mathrm{dt} \\ -q_2 &= -v_b \\ q_2 &= \int \frac{i_b}{C}\ \mathrm{dt} \\ \dot{q}_2 &= \frac{i_b}{C} \\ &= \frac{i_3 + i_4 + i_5}{C} \\ &= \frac{1}{C}\Big(-\frac{\lambda q_2}{R_3} + \frac{\lambda q_1}{R_4} + \frac{(\lambda q_1)(-q_3)}{10\mathrm{V}R_5}\Big) \\ \dot{q}_2 &= \frac{\lambda}{C}\bigg(\Big(\frac{1}{R_4} - \frac{q_3}{10\mathrm{V}R_5}\Big)q_1 - \frac{q_2}{R_3}\bigg) \end{aligned}$$

The dynamics set by v_c:

$$\begin{aligned} v_c &= \int \frac{i_c}{C}\ \mathrm{dt} \\ q_3 &= -v_c \\ &= -\int \frac{i_c}{C}\ \mathrm{dt} \\ \dot{q}_3 &= -\frac{i_6 + i_7}{C} \\ &= -\frac{1}{C}\Big(\frac{\lambda q_3}{R_6} - \frac{\lambda q_1 q_2}{10\mathrm{V}R_7}\Big) \\ \dot{q}_3 &= \frac{\lambda}{C}\Big(\frac{q_1 q_2}{10\mathrm{V}R_7} - \frac{q_3}{R_6}\Big) \end{aligned}$$

The scale for the system is set such that $100\,\mathrm{mV} = 1$ as such $10\,\mathrm{V} = 100$. R_3 is used to set the resistance scale. We select $1\,\mathrm{M\Omega}$ as the base resistance. The system can be rewritten with a change of variable:

$$\hat{R}_i = \frac{1\,\mathrm{M\Omega}}{R_i}$$

Specifically choose $\hat{R}_5 = \hat{R}_7 = 100$

$$R_5 = R_7 = 10\,\mathrm{k\Omega}$$

Using this change along with the scaling set at $100\,\mathrm{mV}$:

$$\begin{aligned}
\dot{q}_1 &= k\lambda(q,m)\hat{R}_1(q_2 - q_1) \\
\dot{q}_2 &= k\lambda(q,m)\big((\hat{R}_4 - q_3)q_1 - q_2\big) \\
\dot{q}_3 &= k\lambda(q,m)\big(q_1 q_2 - \hat{R}_6 q_3\big)
\end{aligned}$$

The value k is then determined as:

$$k = \frac{1}{1\,\mathrm{M\Omega}C}$$

Where C is in Farads. The Lorenz parameters (σ,β,ρ) are set by the scaled resistors $\hat{R}_1, \hat{R}_4, \hat{R}_6$ respectively.

Appendix D

Expanded Figures

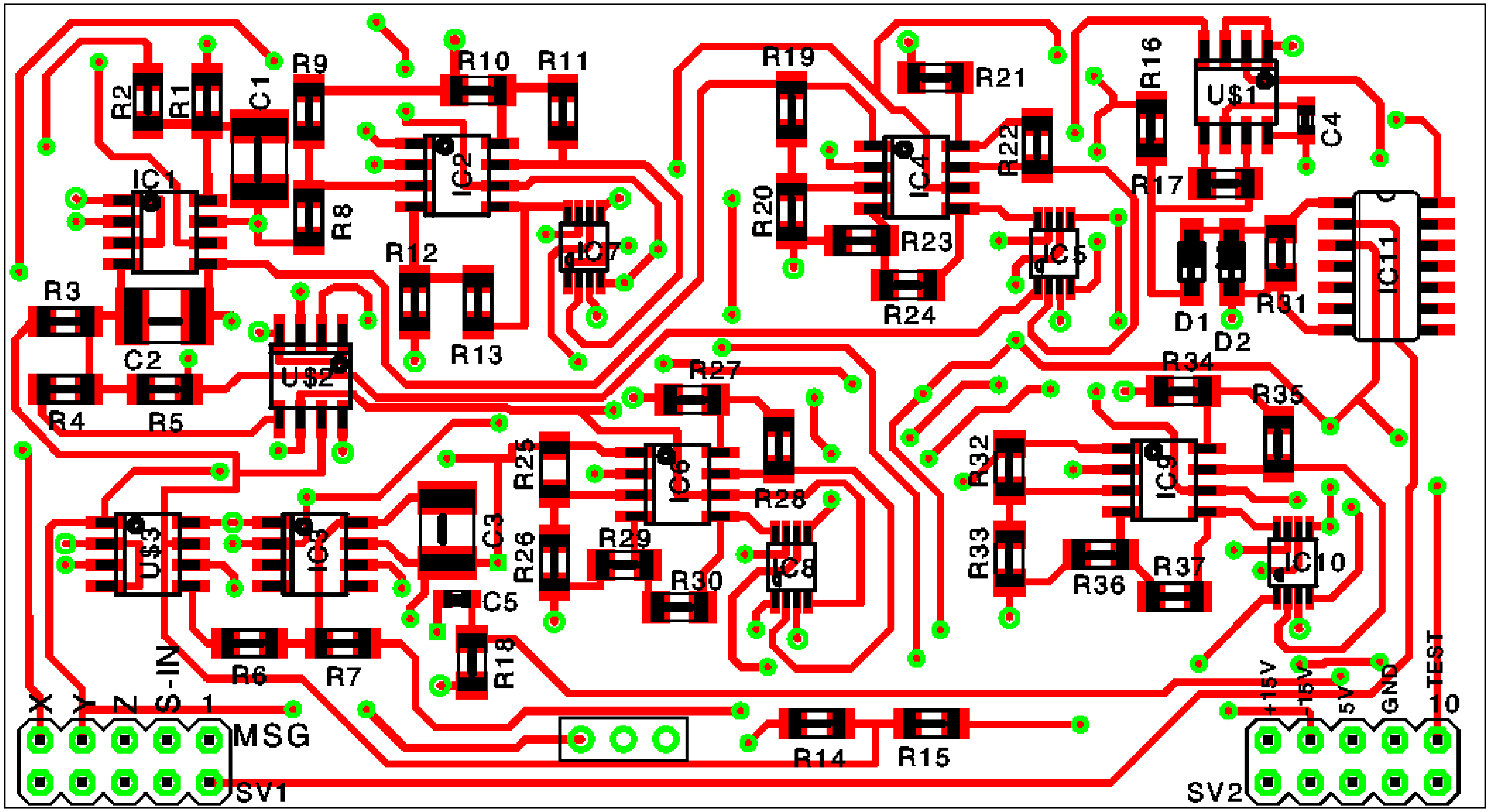


Figure D.1: Expanded View of Figure 3.10a

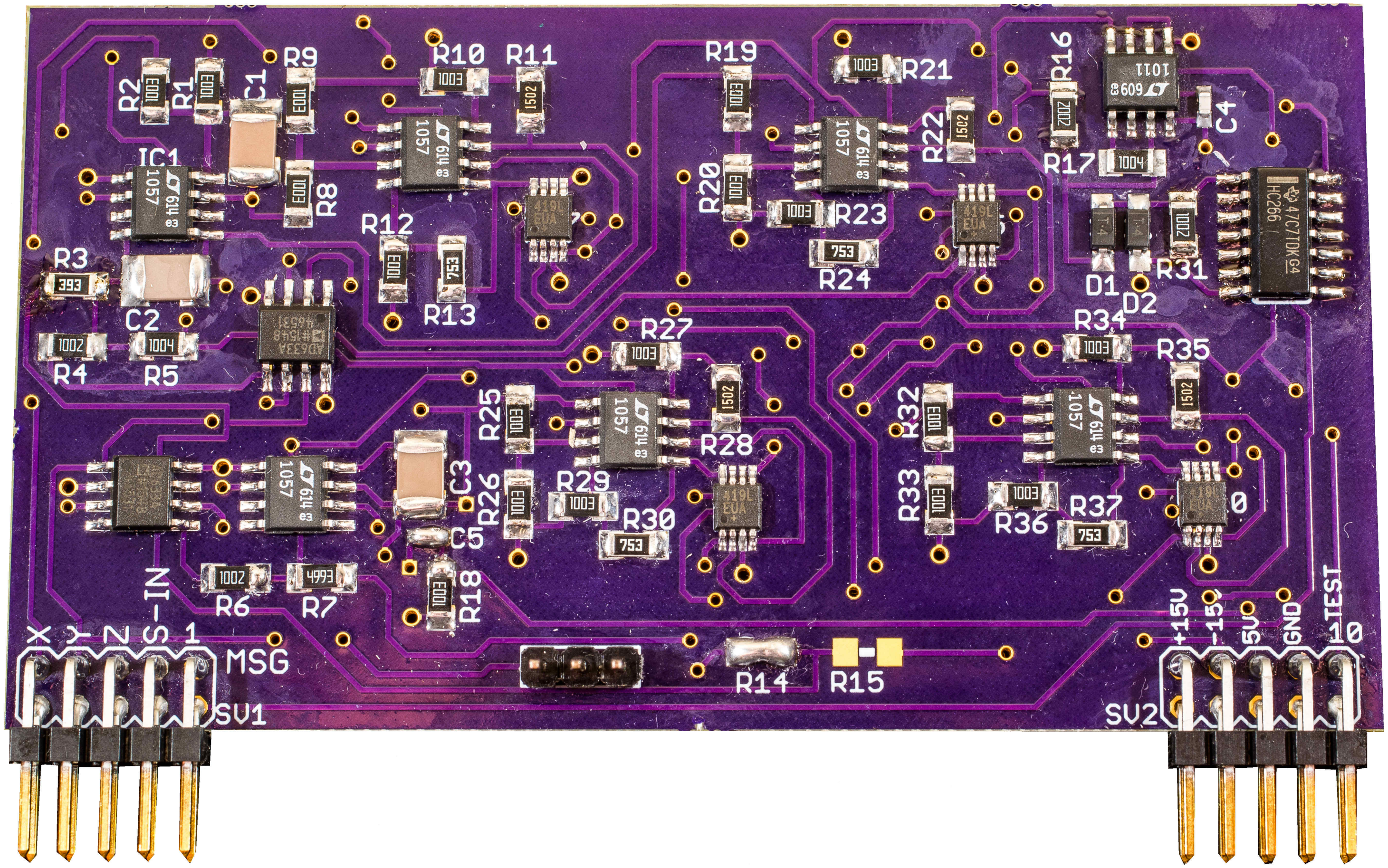


Figure D.2: Expanded View of Figure 3.11a

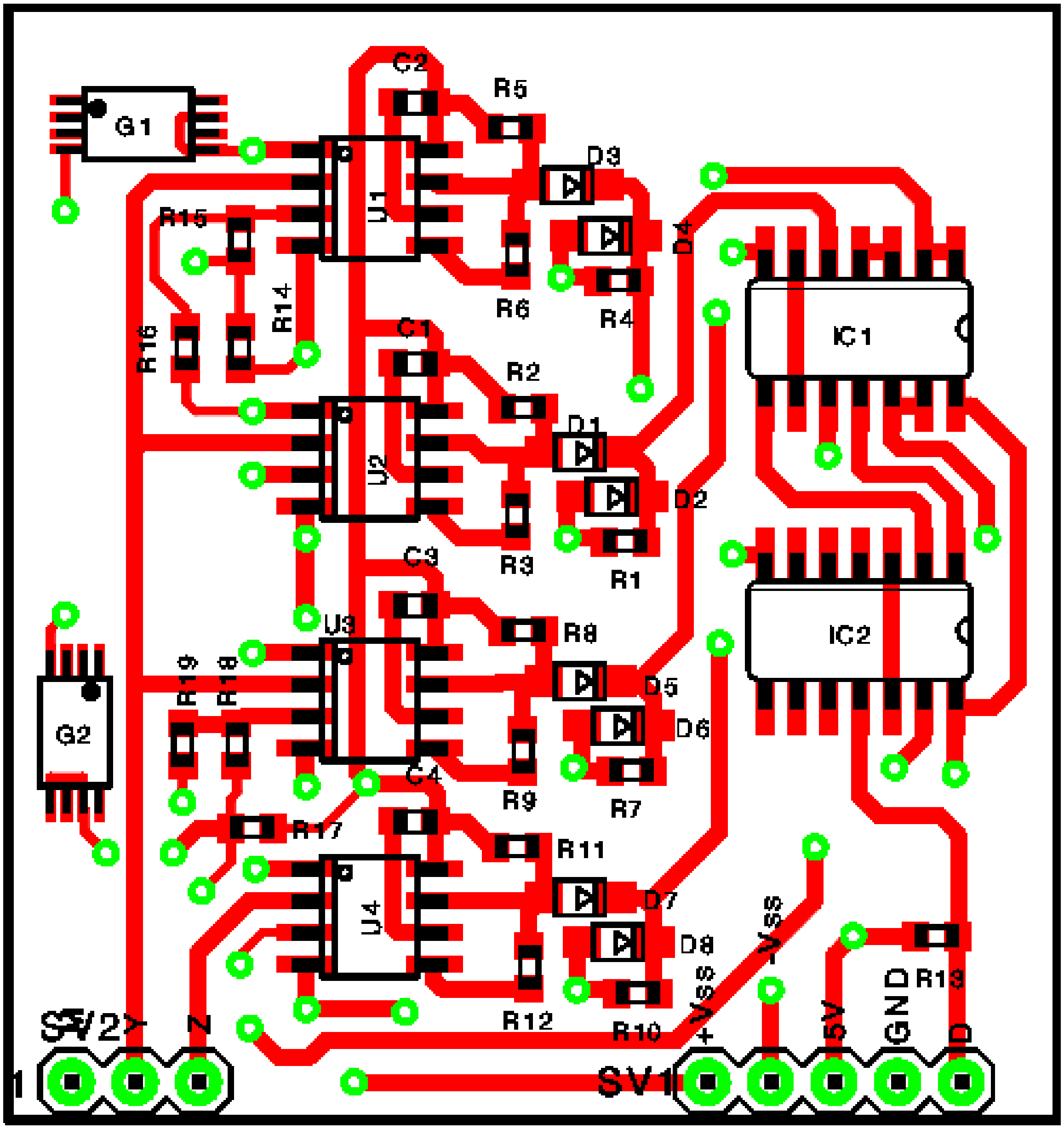


Figure D.3: Expanded View of Figure 3.12a

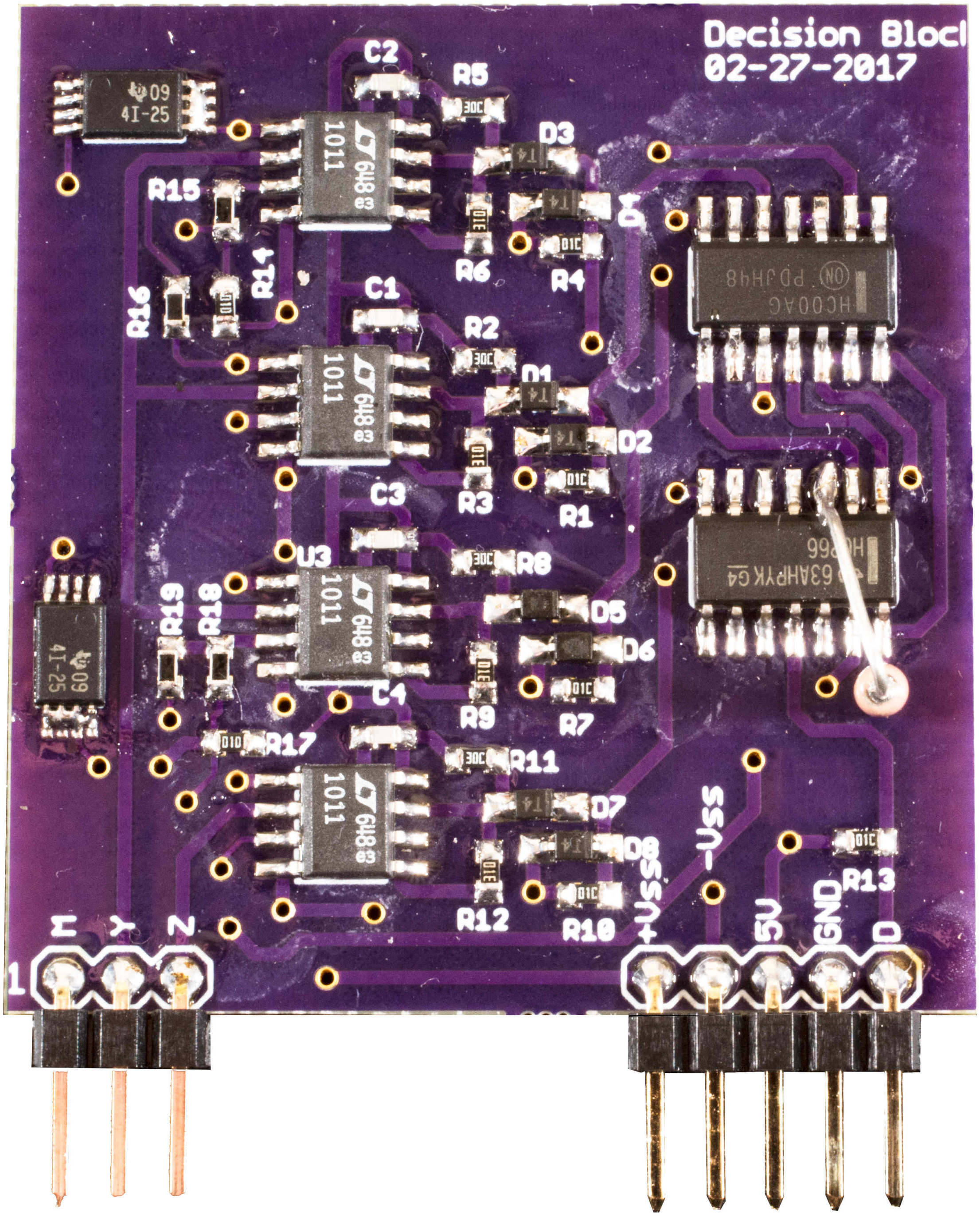


Figure D.4: Expanded View of Figure 3.13a

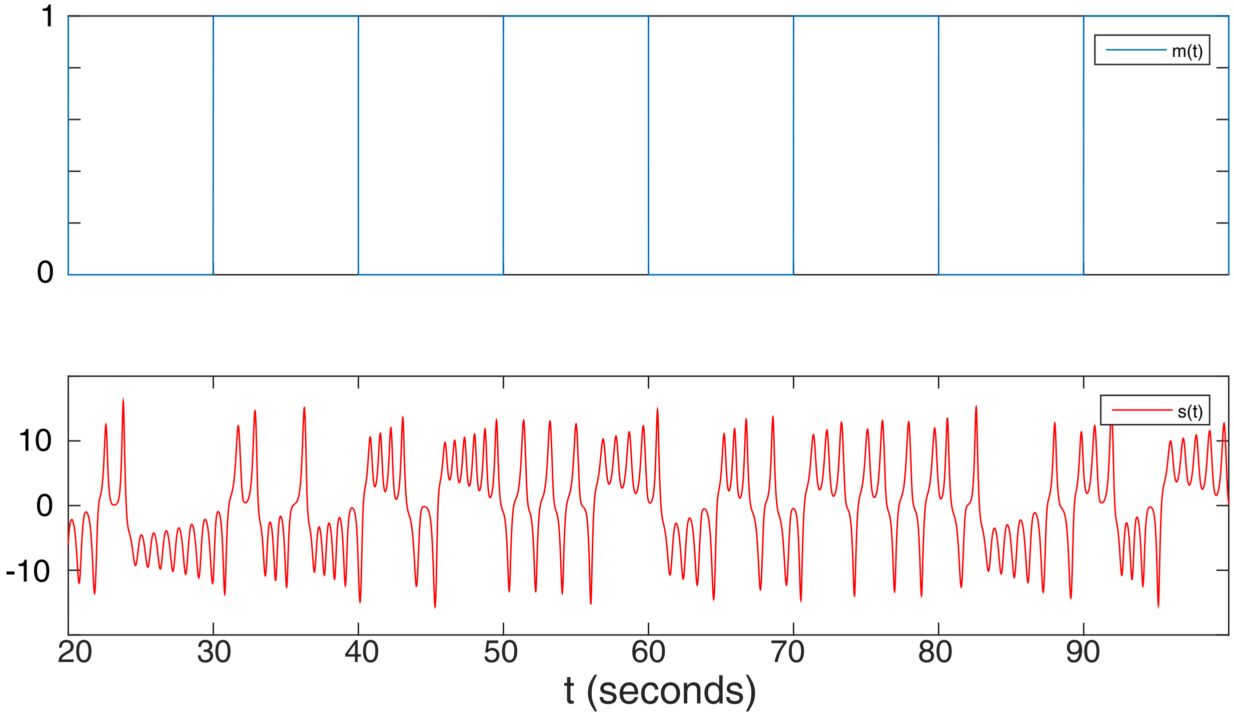


Figure D.5: Expanded View of Figure 4.1a

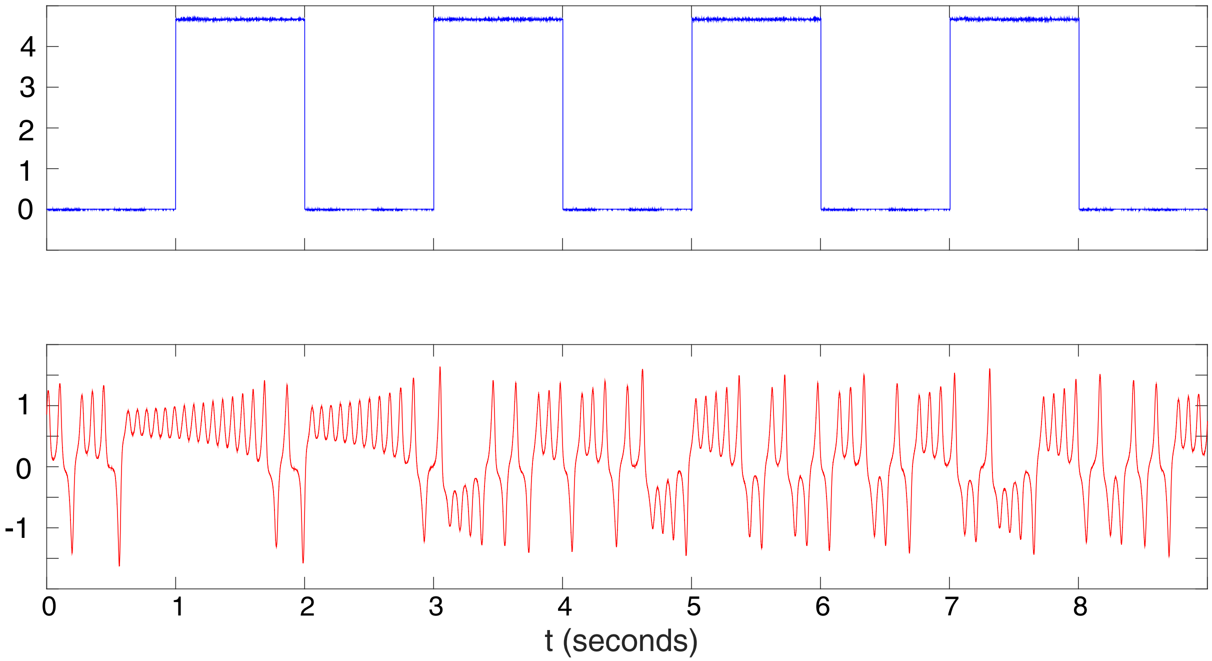


Figure D.6: Expanded View of Figure 4.1b

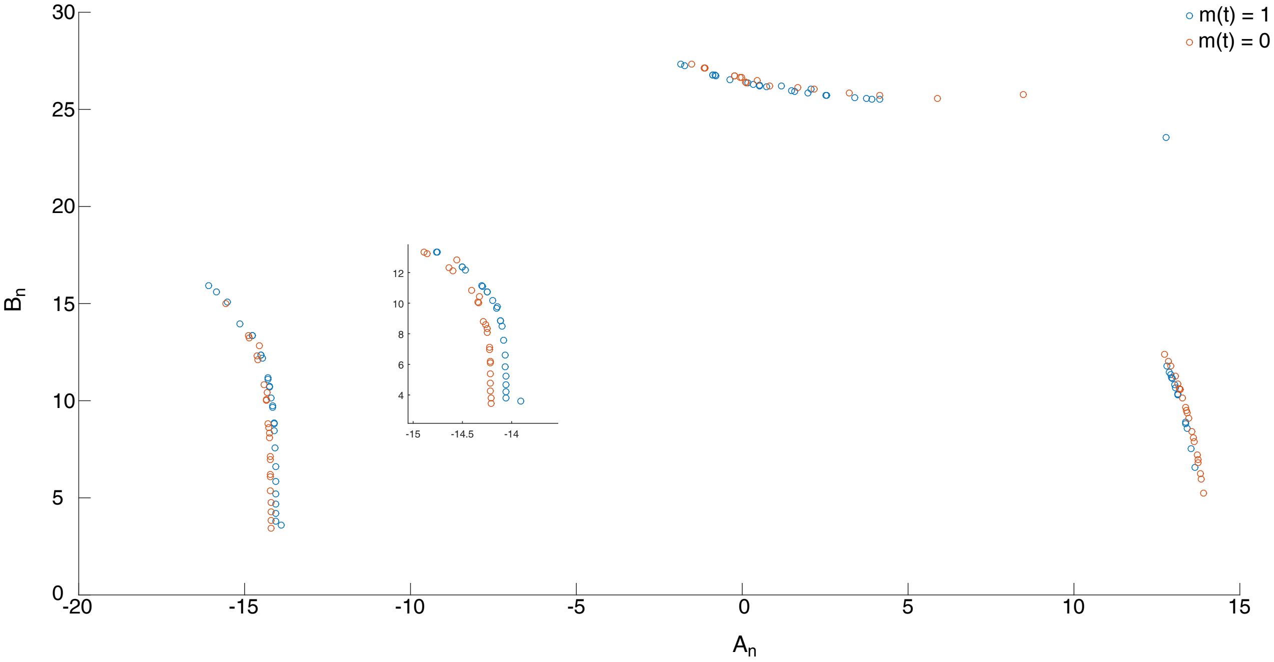


Figure D.7: Expanded View of Figure 4.2a

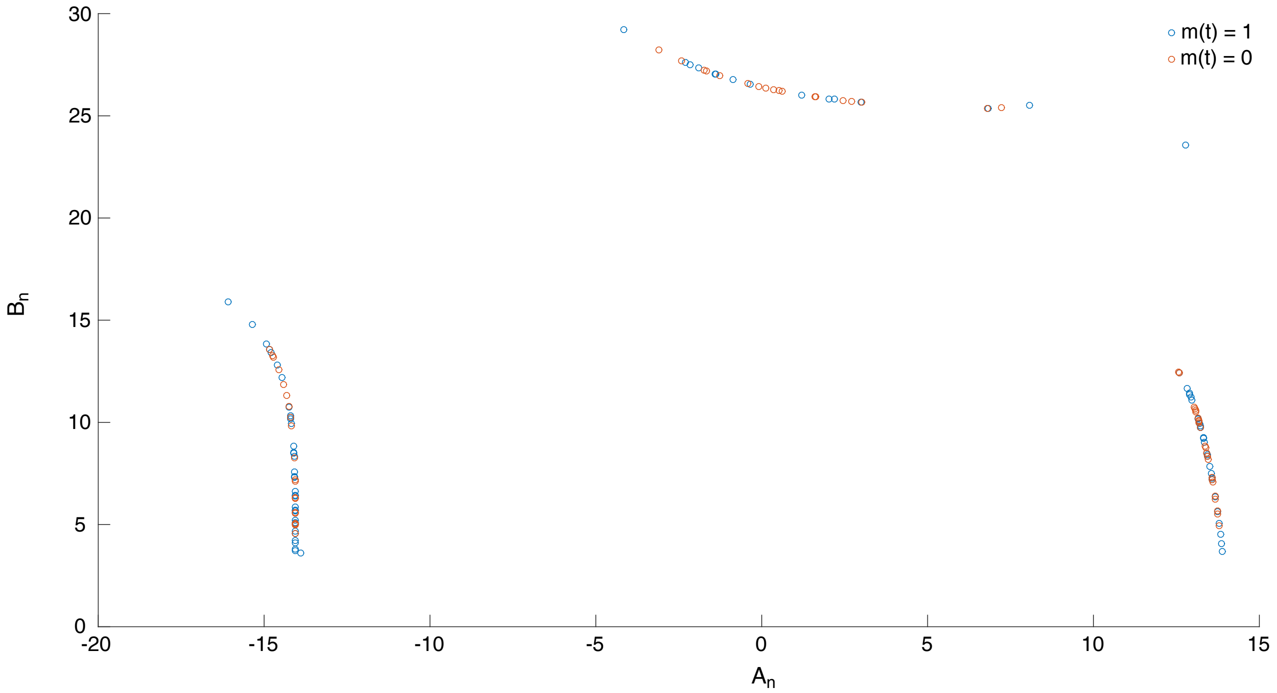


Figure D.8: Expanded View of Figure 4.2b

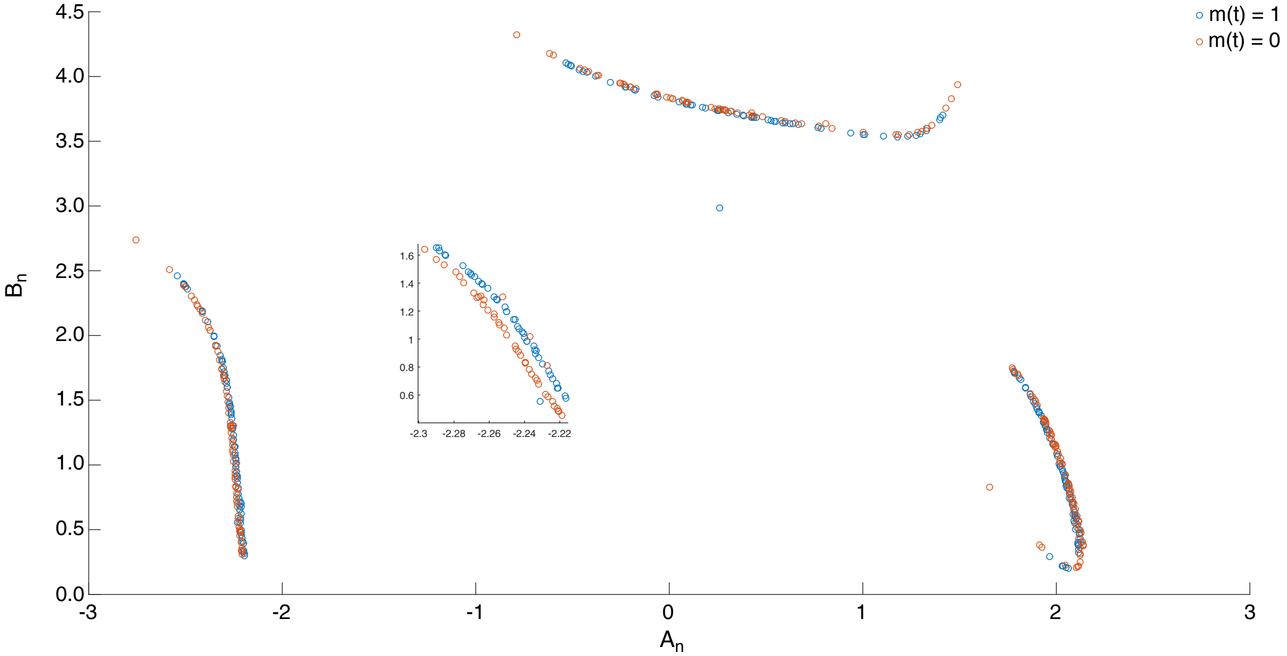


Figure D.9: Expanded View of Figure 4.3a

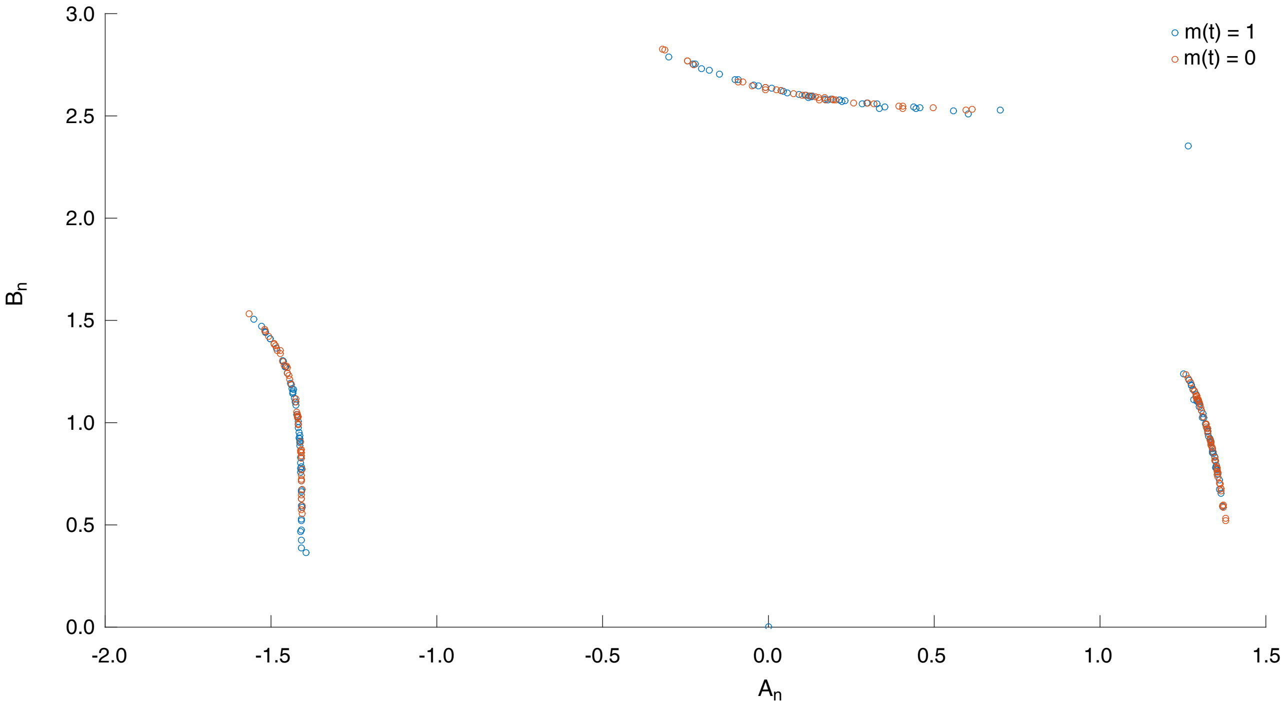


Figure D.10: Expanded View of Figure 4.3b

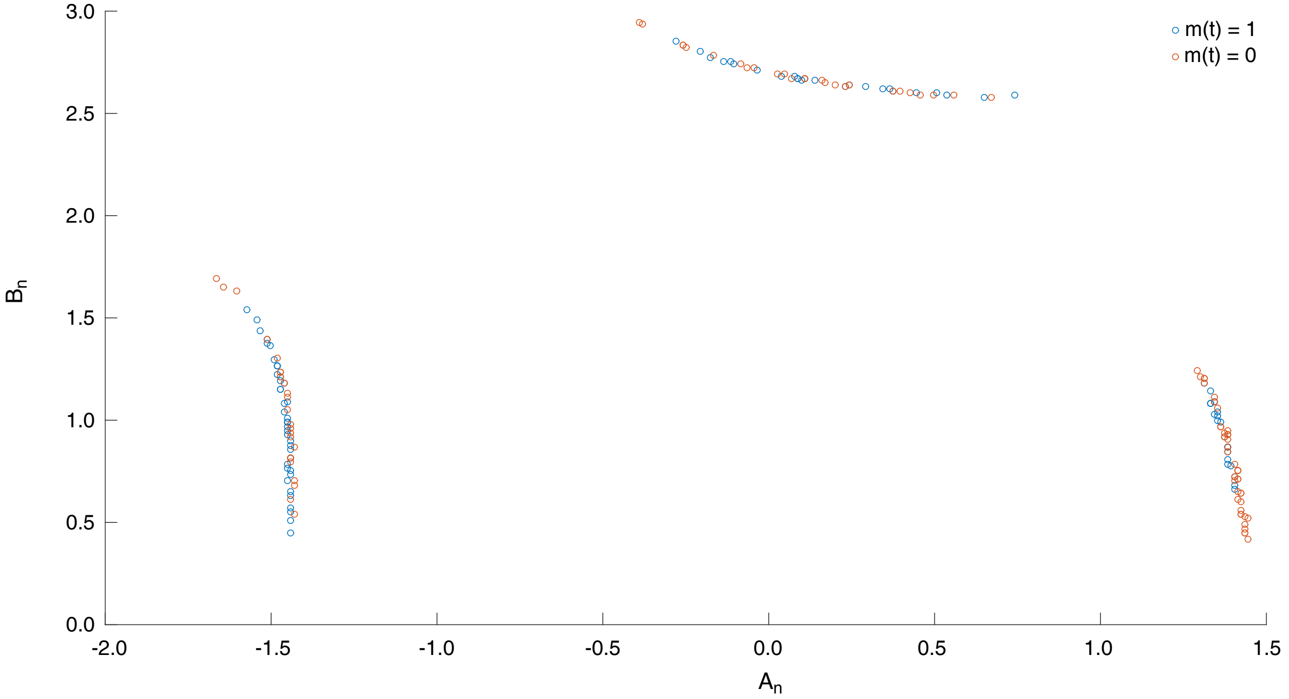


Figure D.11: Expanded View of Figure 4.4

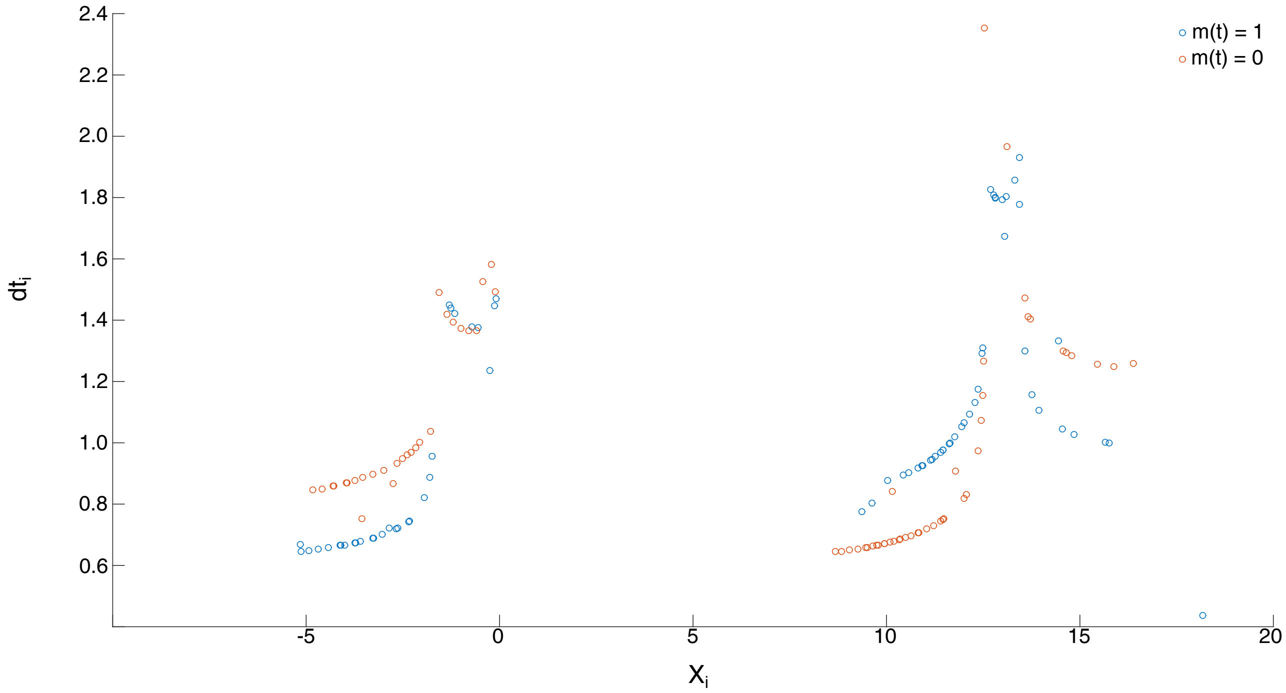


Figure D.12: Expanded View of Figure 4.5a

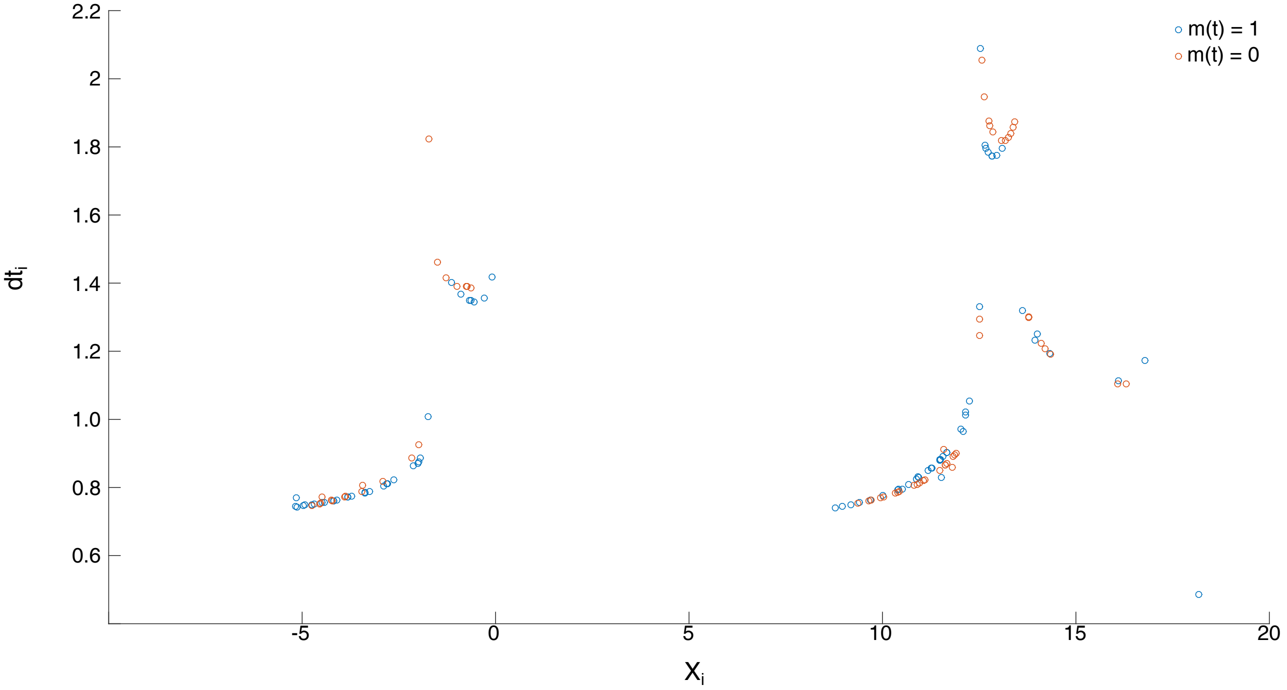


Figure D.13: Expanded View of Figure 4.5b

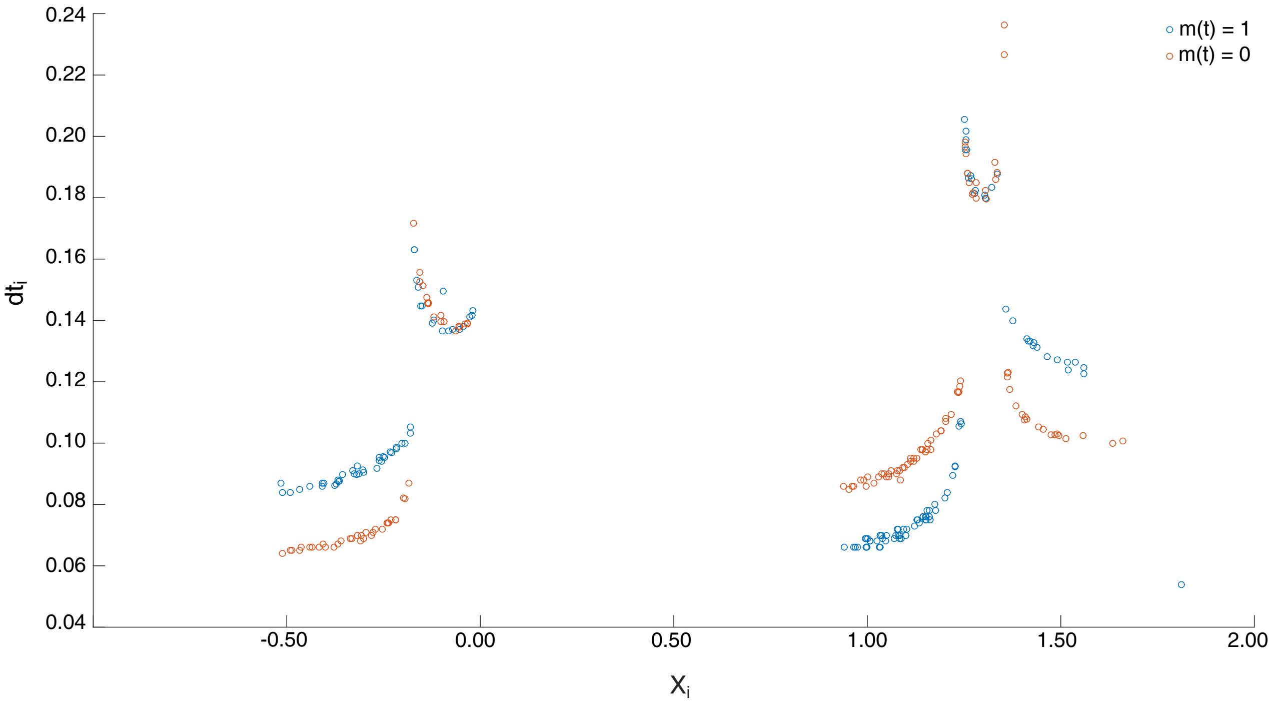


Figure D.14: Expanded View of Figure 4.6a

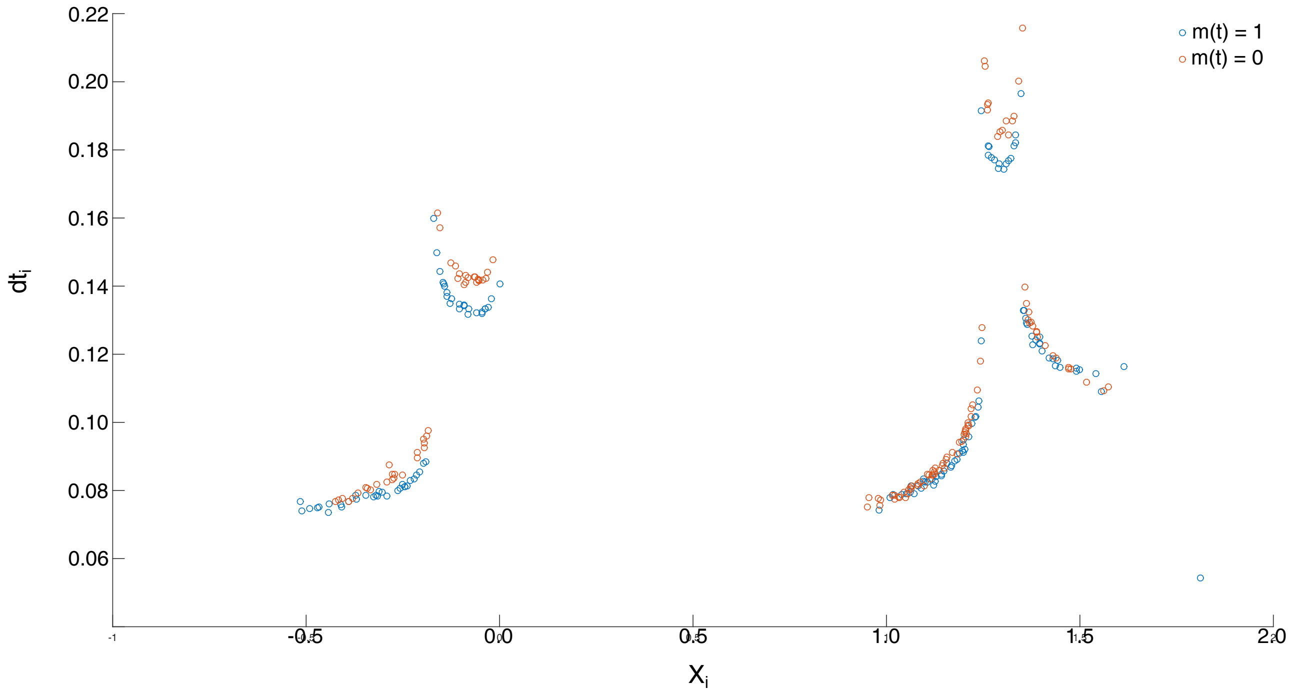


Figure D.15: Expanded View of Figure 4.6b

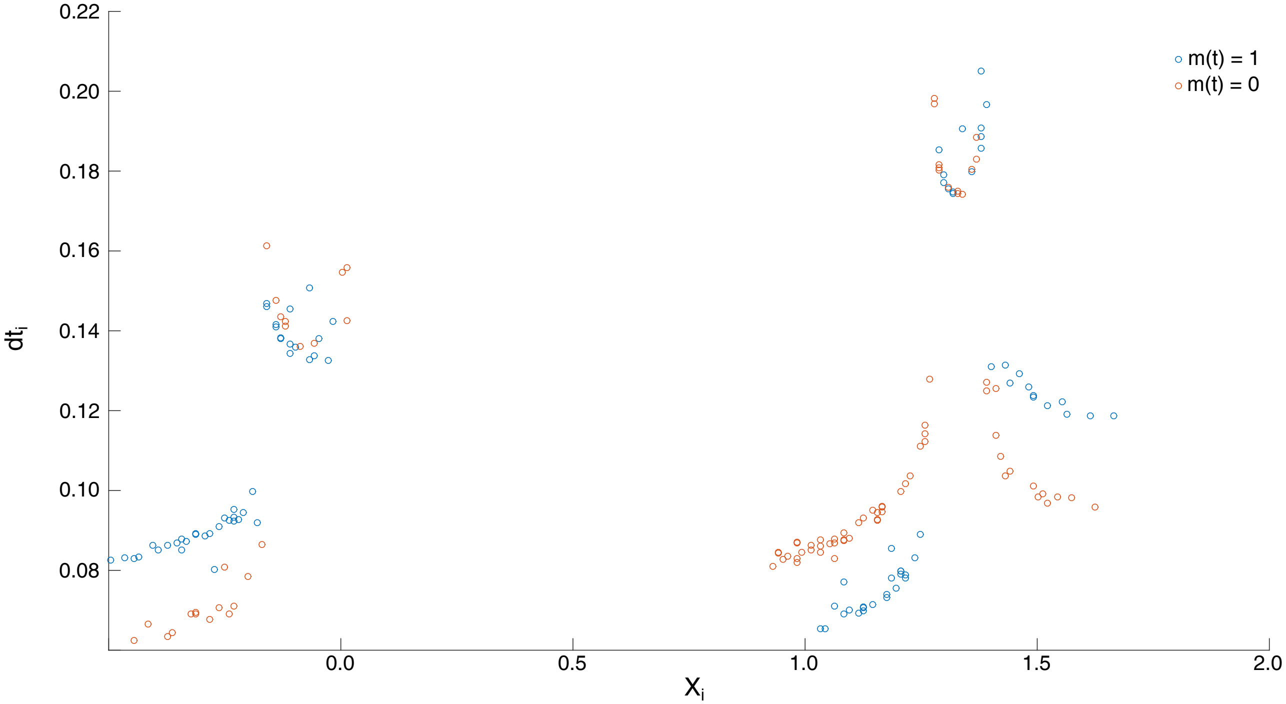


Figure D.16: Expanded View of Figure 4.7a

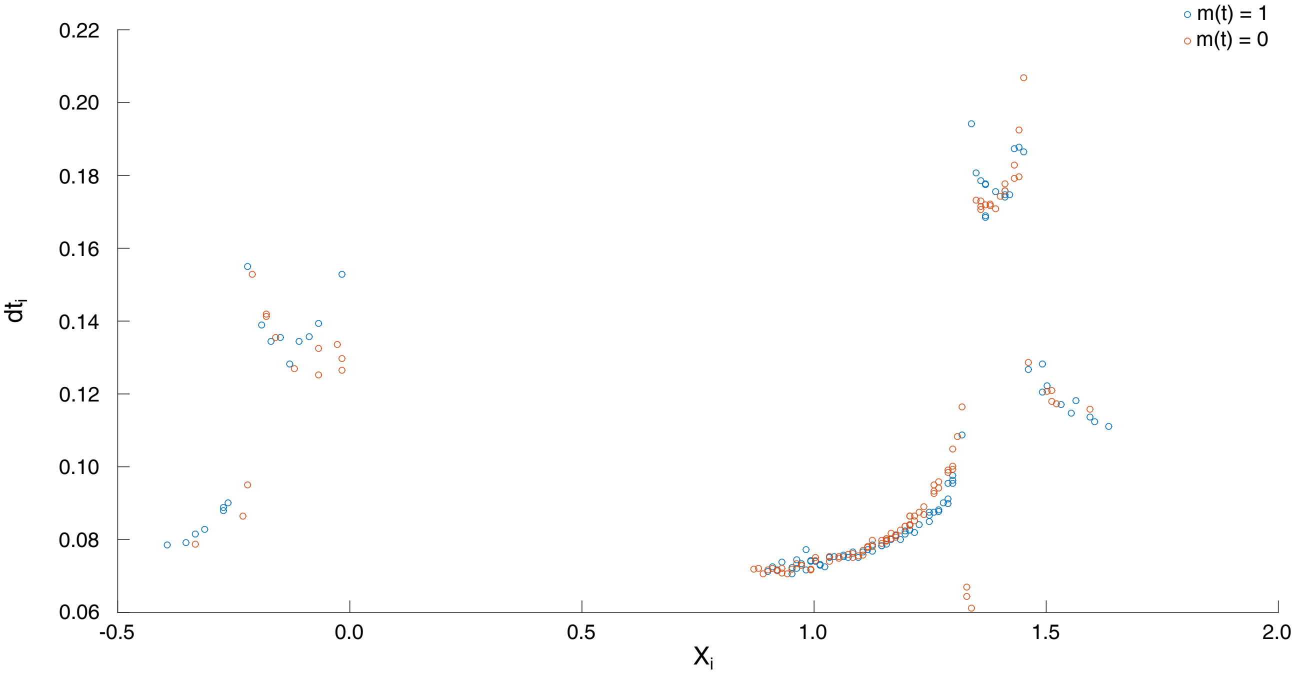


Figure D.17: Expanded View of Figure 4.7b

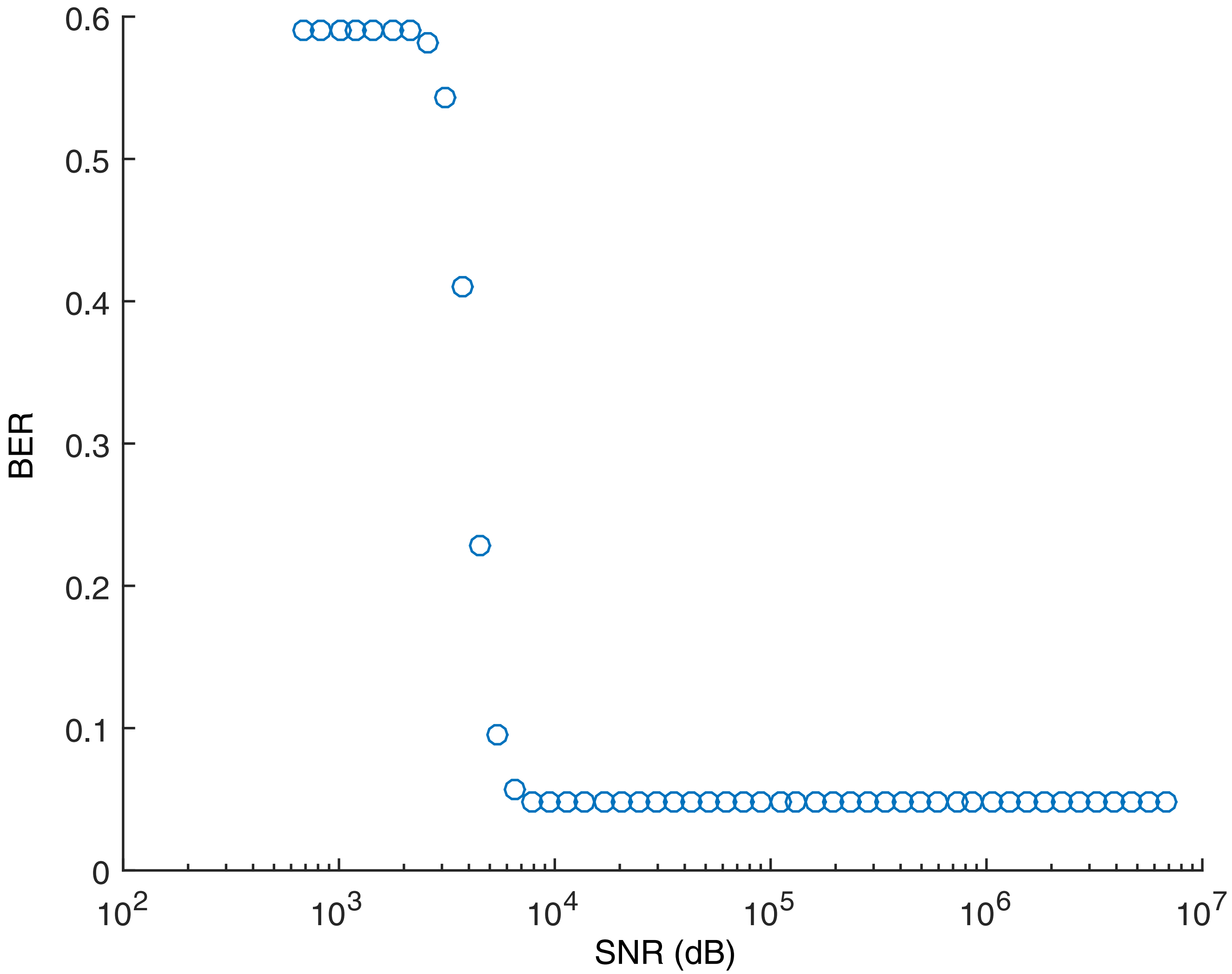


Figure D.18: Expanded View of Figure 4.8

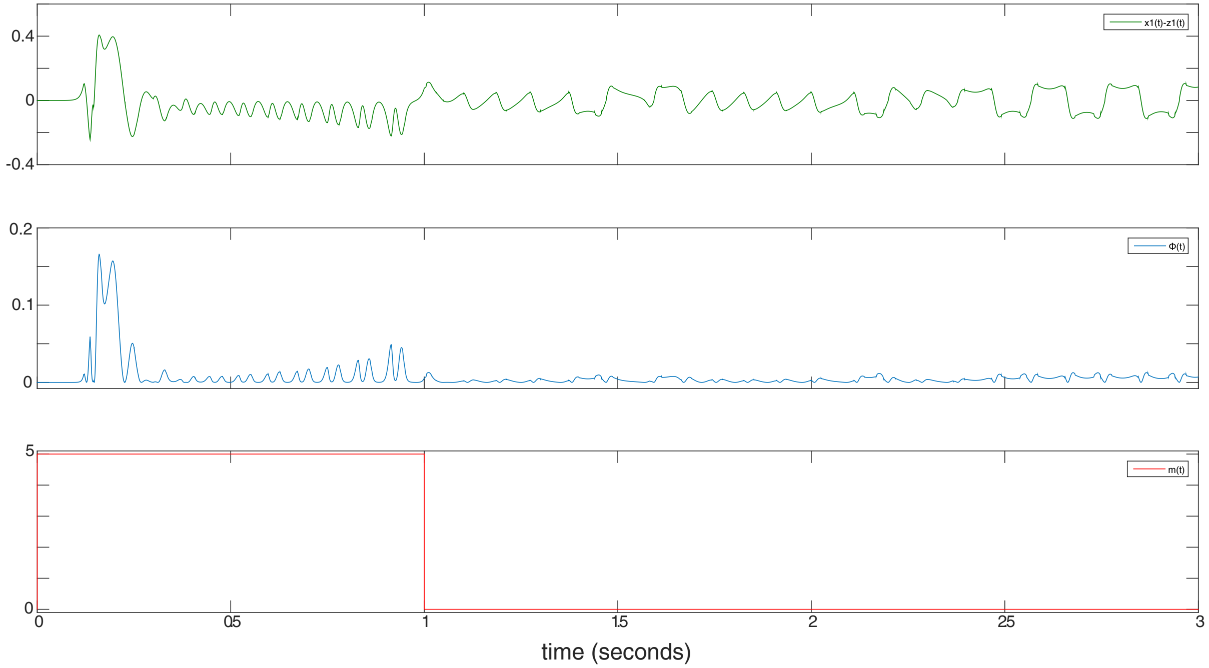


Figure D.19: Expanded View of Figure 4.10

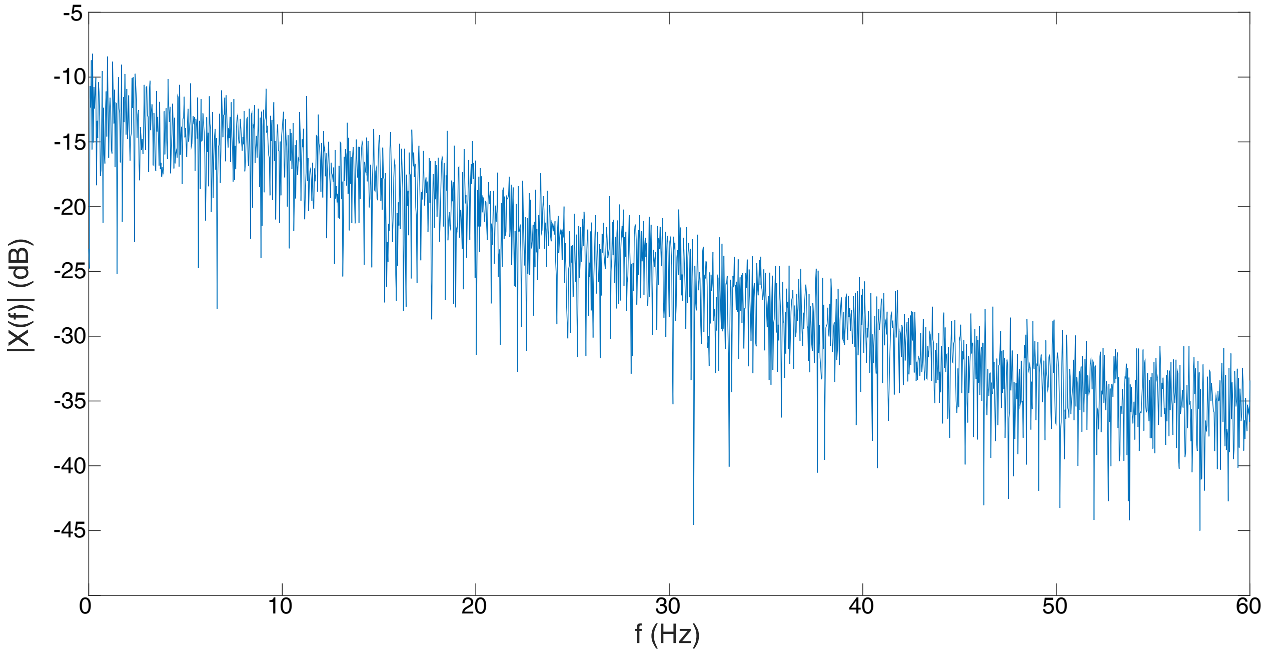


Figure D.20: Expanded View of Figure 4.9a

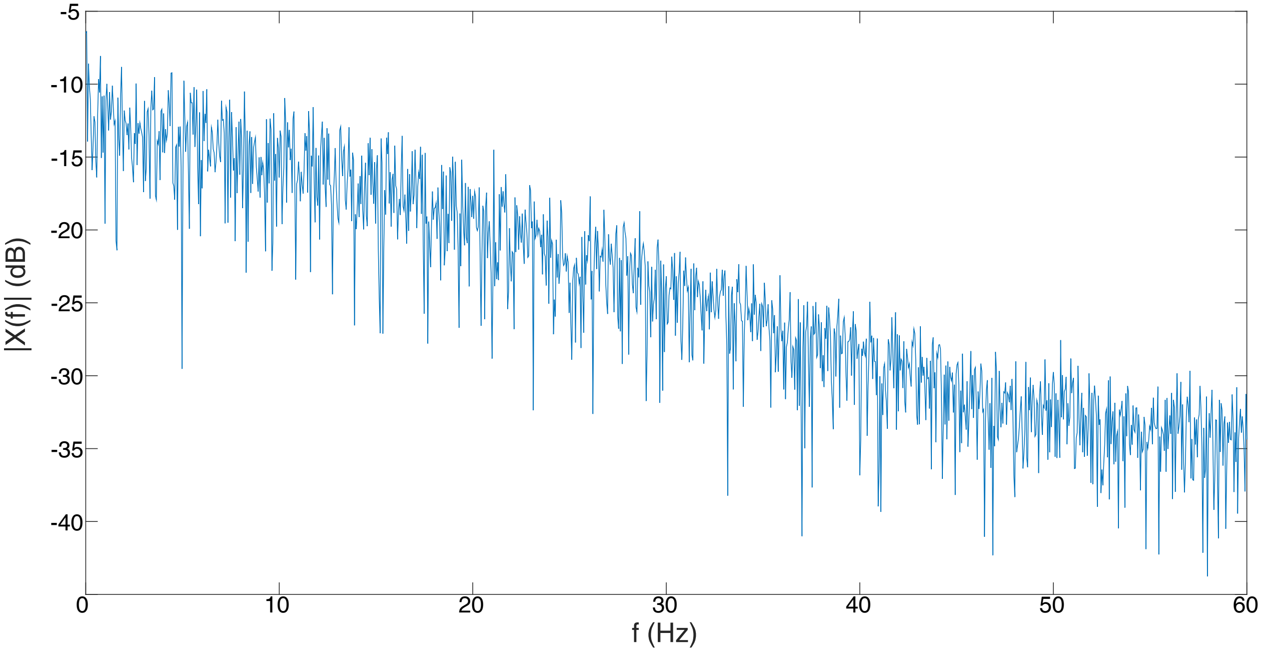


Figure D.21: Expanded View of Figure 4.9b

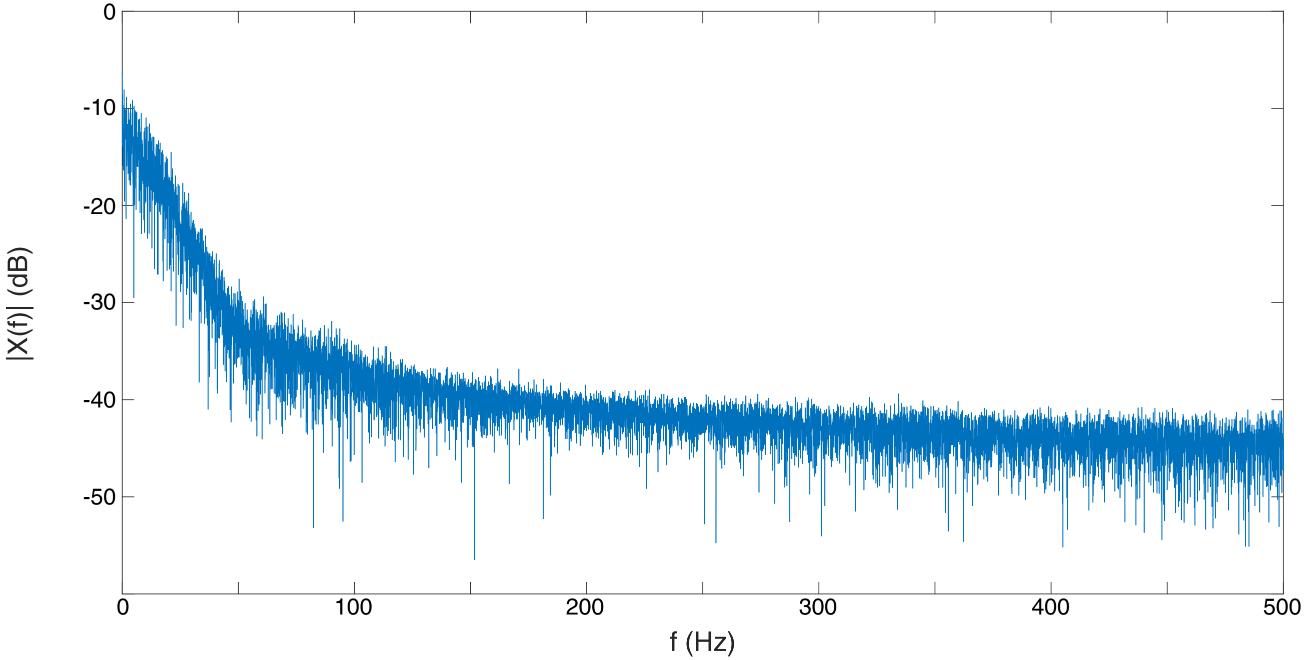


Figure D.22: Expanded View of Figure 4.9c

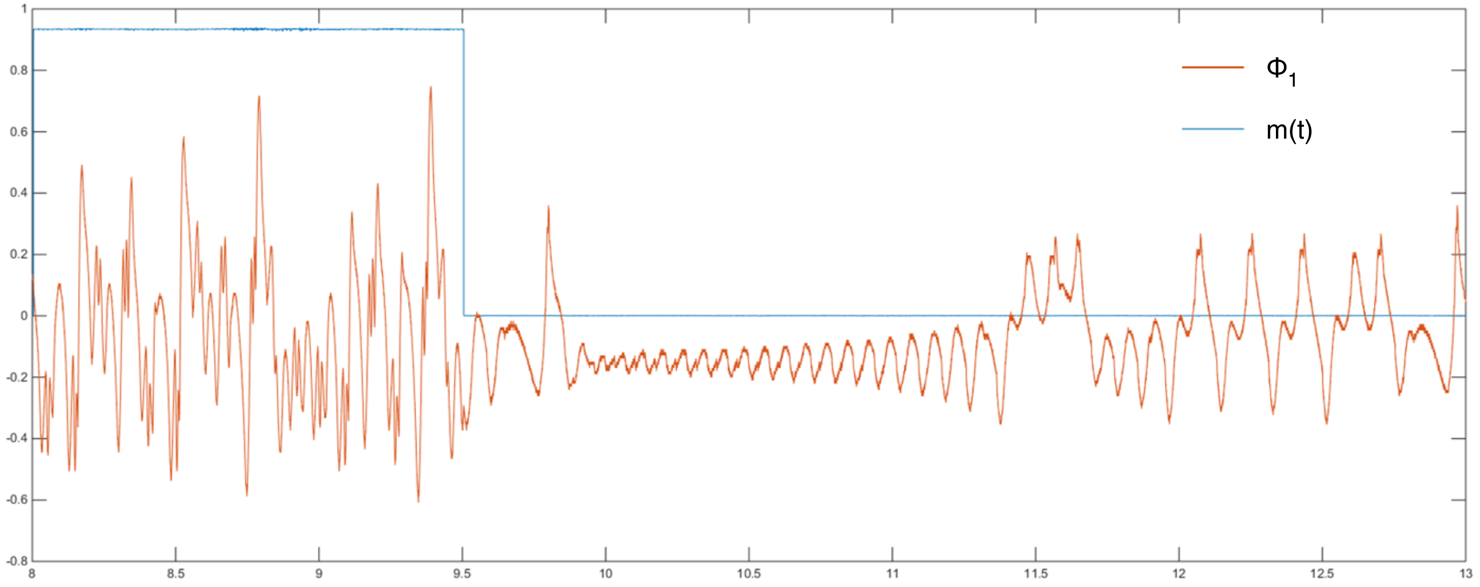


Figure D.23: Expanded View of Figure 5.1

Vita

Daniel Robert Brown was born in Bristol, England, to parents Richard and Suzanne Brown. He is the oldest of three siblings. He graduated from Hershey High School in Hershey, Pennsylvania. He attended Lock Haven University in Lock Haven, Pennsylvania, for his first semester of undergraduate work, later moving to Knoxville, Tennessee. After attending the University of Tennessee for three semesters, he left to attend Pellissippi State Technical Community College (PSTCC) in Knoxville, Tennessee. He received an Associates of Science in Electrical Engineering Technology from PSTCC in 2010. He then began work with the Neutron Optic group of the Oak Ridge National Laboratory where he was encouraged to return to the University of Tennessee. He received his Bachelor's of Science in Electrical Engineering in 2015 with Cum Laude honors. Shortly following graduation Daniel welcomed his first child, Gordon Orion, in June. He then began the pursuit of his Master's of Science in Electrical Engineering the following semester under the guidance of Dr. Donatello Materassi. Daniel is set to graduate May of 2017 with Summa Cum Laude honors with his Master's of Science.