Course: PHY493
Instructor: Dr. Ken Kiers
Date: January 26, 2014

Signal Encryption Using a Chaotic Circuit

Jordan Melendez[1,*]

[1]*Physics & Engineering Department, Taylor University, 236 West Reade Ave., Upland, IN 46989, USA*

Abstract

This paper explores the application of chaotic circuits to the encryption of analog signals. Using nodal analysis, a nonlinear differential equation is derived to model the dynamic behavior of an ideal chaotic circuit. The theoretical predictions made using the ideal differential equation are then compared with experimental data. A transmitting and receiving chaotic circuit are used to encrypt and decode an analog signal, respectively. Because of the circuits' chaotic behavior, the message appears as noise when observed by those without a knowledge of each circuit. Applications and extensions of such a circuit are discussed.

I. INTRODUCTION

Chaos theory is a relatively new science that has gained popularity among people ranging from scientists to the common person. In everyday usage, "chaos" translates roughly to "a state of disarray" or "madness," but in chaos theory the word has a more precise definition. Although not everyone agrees on one definition, chaotic systems are characterized by certain qualities:

1. Sensitivity to initial conditions
2. Nonlinear behavior
3. The error in arbitrarily similar initial conditions grows exponentially with time

The consequence of these qualities is that we cannot predict the future of a chaotic system indefinitely, no matter how well we measure it. Chaos theory puts to rest the possibility of a "clockwork universe," advocated by Pierre Simon de Laplace. Laplace proposed that if you knew the exact state of the universe at a given time, "you could predict its future for all time" [1]. On the contrary, it is impossible for us to predict far into the future for even certain modes of simple systems, such as a dripping tap.

Even completely deterministic systems, like the dripping tap, can yield solutions that are unpredictable. Such behavior often arises in the study of dynamical systems. A dynamical system is a deterministic mathematical prescription for evolving the state of a system forward in time. For discrete systems, a dynamical systems takes the form of mapping functions, while coupled differential equations relate states in a continuous system. In this paper we will focus on the continuous case.

*Electronic address: jordan_melendez@taylor.edu

Most differential equations are not solvable in closed form, in general. This leaves us with the option to use numerical approximation techniques if we want to extract useful information from the set of equations. Without finding an exact solution, we can still use differential equations to give us the prescription to evolve the state of a system into the future for a very short time. Moving the state forward two units of time would require us to repeat, or iterate, the prescription twice. To obtain an accurate prediction into the far future, we would need to use a small time step and iterate the prescription many times. Many tedious calculations are required to perform what, in principle, is a relatively straightforward calculation. Even a century ago, such a task was unfeasible.

Computers are very good at performing millions of arithmetic calculations very quickly. This is why the dawn of high speed computers gave scientists the first glance at chaotic behavior in its entirety. Finally, the ability to predict far into the future was within our grasp, or so we thought. As scientists began to examine certain nonlinear dynamical systems, interesting behavior emerged. They found that some systems have very different long-term behavior, despite arbitrarily similar initial conditions. Even the amount of significant figures held by the computer greatly impacted the possible future for the system. Extreme sensitivity to initial conditions is the trademark of chaotic systems. Because we cannot measure anything with infinite precision, the true future of chaotic systems will always diverge from our predictions given enough time.

Many real world systems can behave chaotically. A few examples include the weather, planetary orbits, coupled pendula, population dynamics, fluid dynamics, and electrical circuits. This corresponds to what we experience on a daily basis. Life, in general, is complicated and uncertain. The future is not easy to predict. Chaos is the gateway from the clockwork, Newtonian universe to the seemingly random and unpredictable universe that we can all relate to.

Despite its unpredictability, there is an order to chaos. Somewhat surprisingly, chaotic systems can be coupled so that they evolve in synchrony. One incredible application of coupled chaotic circuits is to the field of cryptography. This idea has been explored previously using coupled chaotic circuits [2] [3] [4]. Chaotic circuits evolve in seemingly random patterns but coupled chaotic circuits can tell the difference between two "different kinds" of randomness. In one mode, the circuits can synchronize. In the other they cannot. Switching between these two modes can be a sort of message. Because the circuit is behaving effectively randomly, one would not be able to tell the difference in the two modes, in principle. Only with a particular coupled circuit could one determine the synchronous and asynchronous modes and thus, the encrypted message. Each mode can be interpreted as a 0 or a 1 in binary code, which can then be used to reconstruct the message.

In this paper, we examine in detail a simple electrical circuit that can exhibit chaos. To do so, we begin by building a circuit that is modeled by a third-order nonlinear differential equation. First, we will derive the theoretical model using nodal analysis and assess the accuracy of its predictions. Second, we will couple two "identical" chaotic circuits in an attempt to hide binary signals amongst the chaos. The speed and accuracy of the decryption mechanism will be analyzed. Finally, we will conclude with possible extensions of our work.

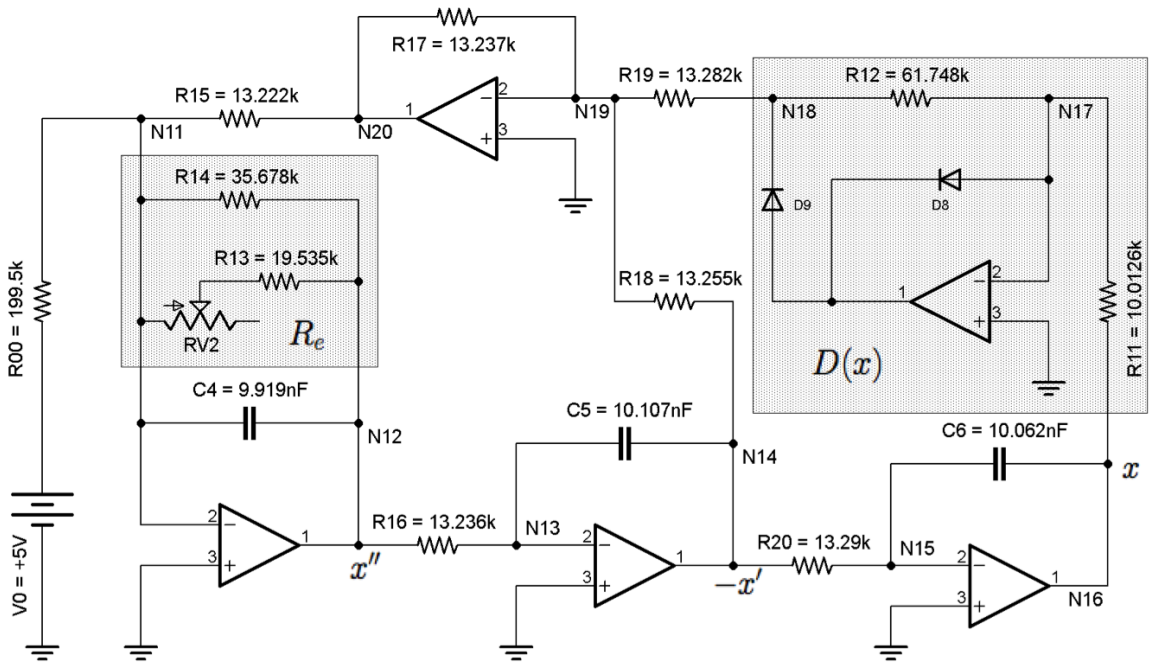


FIG. 1: The chaotic circuit described in [5]. Depending on the value of R_e, the circuit displays either periodic or chaotic behavior. Ideally, $R = R_i = 13.23\text{k}\Omega$ for $15 \leq i \leq 20$ and $C = C_j = 10\mu\text{F}$ for $4 \leq j \leq 6$. Primed variables represent derivatives with respect to the dimensionless variable $\tau = t/RC$.

II. ANALYSIS

A. The Circuit

To exhibits chaos, a circuit must include components that cause nonlinearity. We use a relatively simple circuit, described in [5]. This circuit contains three integrating op-amps, a summing op-amp, and a subcircuit, $D(x)$, which contains an arrangement of diodes and another op-amp. The nonlinearity of the circuit is derived from the subcircuit, $D(x)$. $D(x)$ compares the voltage x to ground and takes the minimum.
Quantitatively,

$$D(x) = -\frac{R_{12}}{R_{11}} \min(x, 0). \qquad (1)$$

Using nodal analysis examined in the Appendix, we can determine that the differential equation has the form

$$\dddot{x} = a_1\ddot{x} + a_2\dot{x} + a_3 D(x) + a_4, \qquad (2)$$

where $\dot{x} = dx/dt$. If we treat each resistor as distinguishable and use the number scheme in Fig. 1, it can be shown that

$$\begin{aligned} a_1 &= -\frac{1}{R_e C_4}, \\ a_2 &= -\frac{R_{17}}{R_{15}R_{16}R_{18}C_4C_5}, \\ a_3 &= \frac{R_{17}}{R_{15}R_{16}R_{19}R_{20}C_4C_5C_6}, \\ a_4 &= -\frac{1}{R_{00}R_{16}R_{20}C_4C_5C_6}V_0, \end{aligned} \qquad (3)$$

where

$$R_e = \left(\frac{1}{R_{14}} + \frac{1}{R_{13} + R_{v_2}}\right)^{-1}. \qquad (4)$$

If we include the additional simplifica-

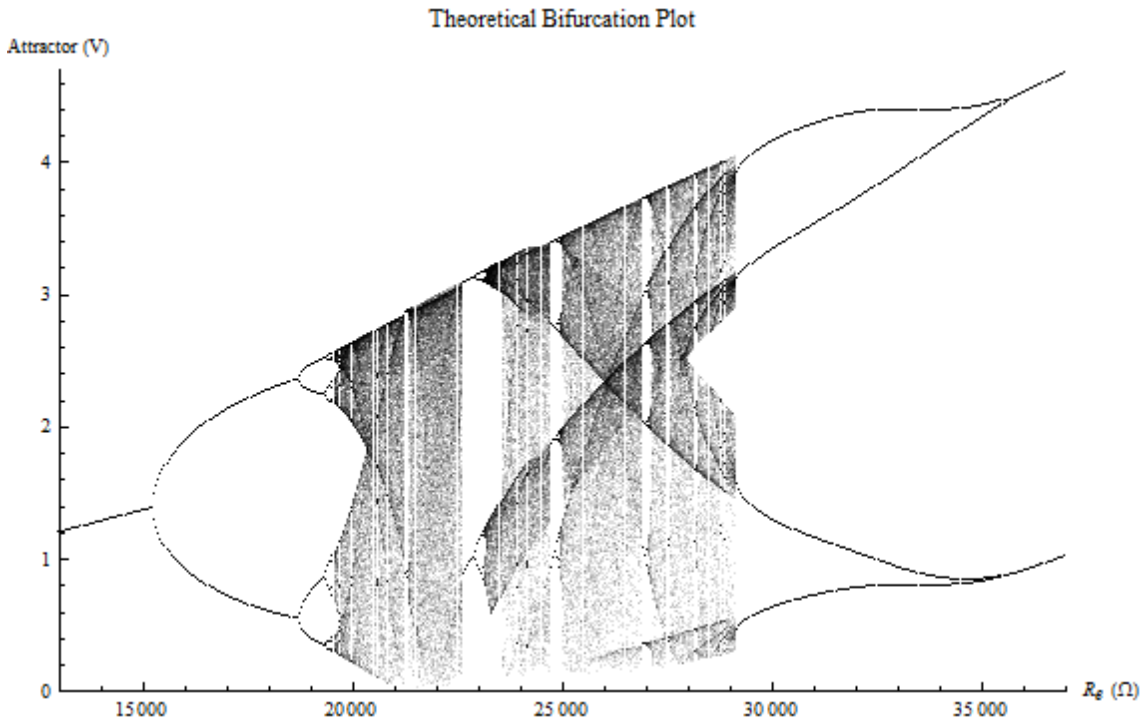


FIG. 2: Bifurcation plot for the parameter R_e. The circuit follows a period doubling route to chaos. Because $0 \leq R_{v_2} \leq 100\text{k}\Omega$, $13 \leq R_e \leq 28\text{k}\Omega$ for our circuit.

tions

$$\begin{aligned} R &\equiv R_{15} = R_{16} = R_{17} \\ &\equiv R_{18} = R_{19} = R_{20}, \\ C &\equiv C_4 = C_5 = C_6, \\ \tau &\equiv \frac{t}{RC}, \\ x' &\equiv \frac{d}{d\tau}, \end{aligned} \tag{5}$$

the model simplifies to

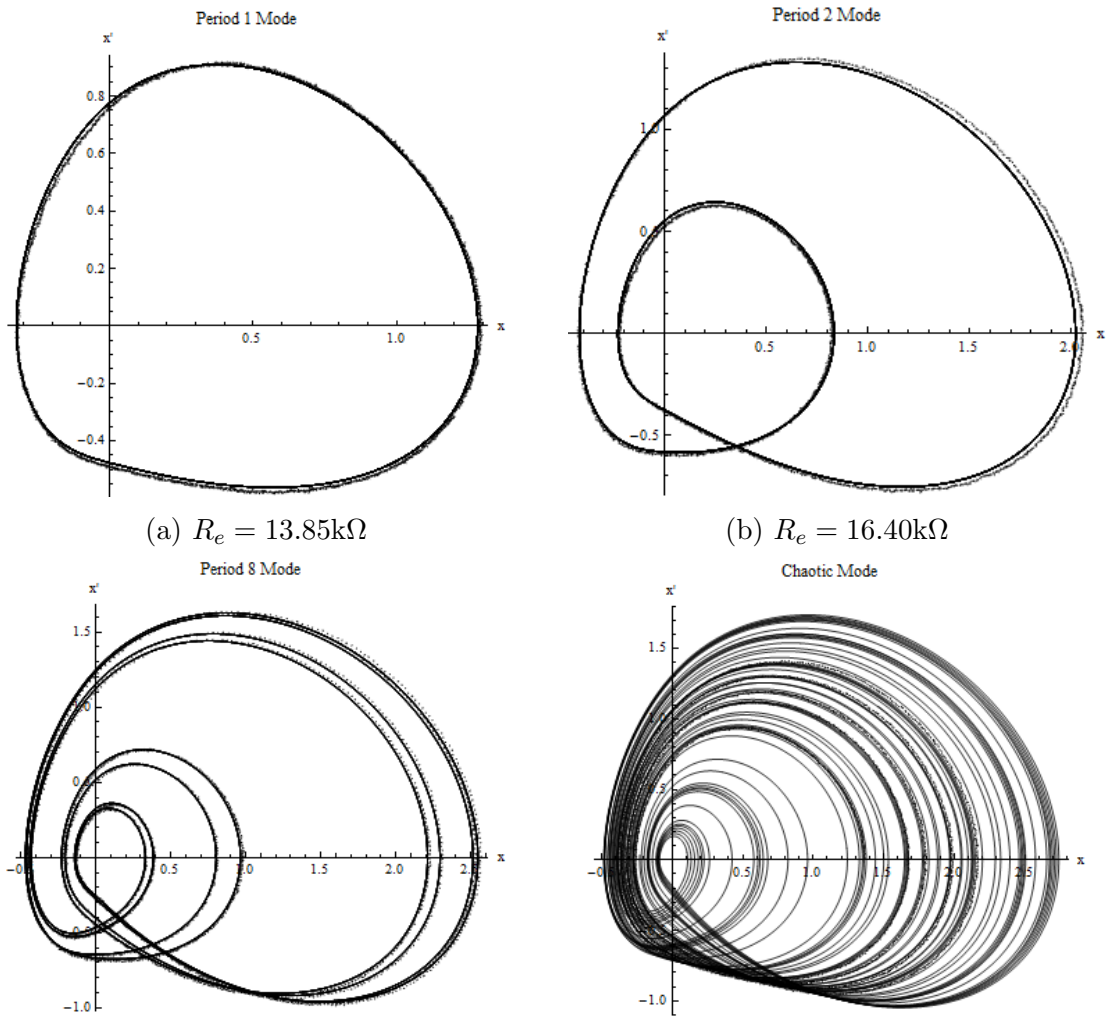
$$x''' = -\frac{R}{R_e}x'' - x' + D(x) - \frac{R}{R_{00}}V_0, \tag{6}$$

which agrees with [5]. R_{11} and R_{12} are chosen so that $R_{12}/R_{11} \approx 6$.

It is the equivalent resistance, R_e, that determines the behavior of the circuit. For certain values, the circuit varies periodically, while for others it is chaotic. Figure 2 sums up the transitions from periodicity to chaos in a bifurcation plot. Experimental bifurcation values were gathered and compared to the predictions made by Fig. 2. This analysis is shown in Table I. Agreement between theory and experiment is exceptional, with no percent error over .4%. Other bifurcations beyond the period 8 to period 16 transition were experimentally indistinguishable from chaos.

Period	Exp. (kΩ)	Theory (kΩ)	% Error
$1 \rightarrow 2$	15.16	15.22	.379
$2 \rightarrow 4$	18.62	18.68	.354
$4 \rightarrow 8$	19.28	19.34	.357
$8 \rightarrow 16$	19.42	19.48	.299

TABLE I: Theoretical and experimental bifurcation points. All legible bifurcation points agree to within .4%.



(a) $R_e = 13.85\text{k}\Omega$ (b) $R_e = 16.40\text{k}\Omega$

(c) $R_e = 19.40\text{k}\Omega$ (d) $R_e = 20.58\text{k}\Omega$

FIG. 3: Experimental phase portraits (dots) overlaid with theoretical phase portraits (lines). Measured values for R_e were used for theoretical predictions with the results showing incredible agreement. Both x and x' are in volts.

Phase portraits of x' vs x were generated experimentally using an oscilloscope and theoretically using Mathematica. A data smoothing algorithm in Mathematica cleaned up our experimental data points and allowed for better agreement with theory. The accuracy of our model and the precision with which each circuit component was measured yielded great agreement between theory and experiment. Results are shown in Fig. 3.

The accuracy of our model is due in great part to the fantastic job that the subcircuit, $D(x)$, does at modeling Eq. (1). As can be seen in Fig. 4, Eq. (1) yields a very accurate representation of the experimental results.

B. Experiments in Cryptography

Contrary to what one first might expect, chaotic systems can become synchronized. If two or more identical chaotic systems are coupled, they can

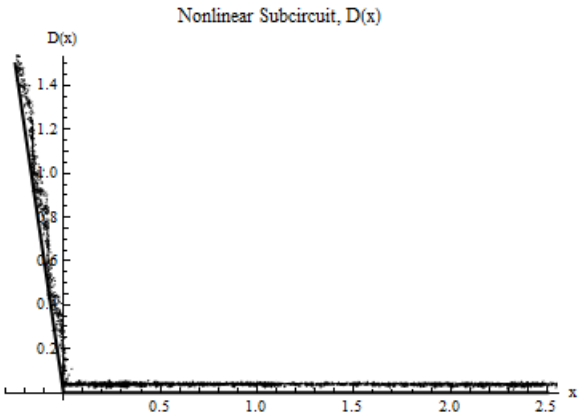


FIG. 4: Experimental measurement of the function $D(x)$. $D(x)$ and x are in volts.

evolve identically with time. This phenomenon is known as complete synchronization.

Complete synchronization can be utilized to encrypt signals. Because chaotic systems are so unpredictable, decoding a message from a chaotic signal may at first seem like a lost cause. As shown in [2], [3] and [4], cryptography through chaotic circuits is possible, but due to speed and accuracy predictions, it may not be practical. Whether or not two circuits are completely synchronized or not can be interpreted as a 1 or a 0, respectively. To completely synchronize two chaotic circuits, they must be identical and coupled. Thus we built and coupled two nearly identical circuits: a transmitter and receiver.

Coupling the transmitter and receiver while analyzing their synchronization state took a complex connection of many subcircuits. All of the relevant circuit diagrams can be seen in Fig. 8. A more detailed explanation of the circuit in its entirety is given in Appendix B.

The transmitting and receiving circuits function similarly to the circuit in Fig. 1. Each circuit has a minor but important difference. The circuit diagrams for the transmitter and receiver can be seen in Figs. 8a and 8f, respectively. Before the details are discussed, we must adjust our current notation. Following the notation in Fig. 1, let $x \to x_1$ for the transmitting circuit and $x \to x_2$ for the receiver.

The first difference is related to the way in which the transmitter and receiver are coupled. The coupling manifests itself in the voltage that is fed to the nonlinear subcircuit of the receiver. Rather than receiving a voltage of x_2, the coupling circuit shown in Fig. 8e is used to feed $D(x)$ a voltage of approximately $.8x_1 + .2x_2$ instead. This couples the transmitter and receiver so that the state of the receiver is affected by the state of the transmitting circuit.

In the transmitting circuit, R_{v_2} is replaced with a more complicated arrangement of resistors and transistors labelled R_T. R_T can switch between two discrete resistance values that are controlled by an Arduino. In one mode, the receiving circuit completely synchronizes with the transmitter, while in the other it does not. These two modes can most clearly be distinguished when one examines the difference $x_2 - x_1$. In the synchronized mode, their difference has a very small amplitude. When unsynchronized, $x_2 - x_1$ has a larger amplitude.

In any communication situation that one could conceivably consider realistic, the transmitter and receiver are connected to different power sources. An encoded message is more useful when it is sent many miles away as opposed to when the transmitter and receiver are only a few inches apart. To build a circuit that could send a signal between two power sources that had been offset by a voltage, V_d, was one of our main priorities.

To make the potential offset essentially irrelevant, we employed a method known as differential signaling. A pair

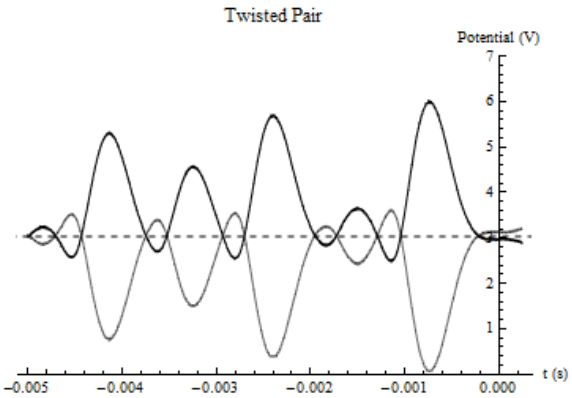


FIG. 5: Experimental twisted pair: $x + V_d$ and $-x + V_d$. The transmitter is offset by $V_d \approx 3$V. The ordinate axis is defined relative to the receiver's ground.

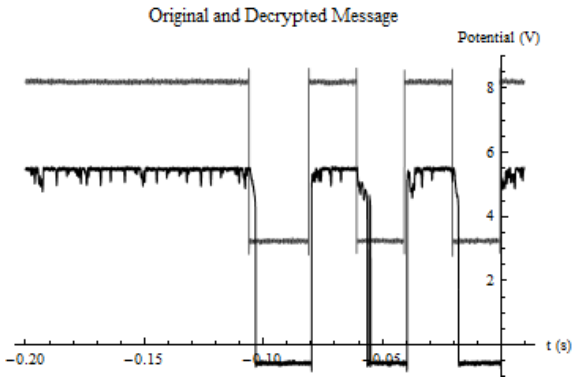


FIG. 6: Original binary signal (gray) plotted against the decrypted signal (black). The 3V offset is evident, yet the signal is decrypted accurately.

of signals is sent from the transmitter, $x + V_d$ and $-x + V_d$, as can be seen in Fig. 5. On the receiving end, the difference of the pair taken with respect to the receiver's ground, g_2. This yields $2x$, which can then be halved to obtain x relative to the new ground. The circuit that performs these operations can be seen in Fig. 8c.

The signal, x_1, can then be accurately compared to x_2 via their difference $x_2 - x_1$. The difference is then transformed into a binary signal using an ideal absolute-value circuit, low pass filter and comparator. Finally, the signal reaches an Arduino, which then reads the digital signal and translates it back into a meaningful message. Figure 8d shows the many subcircuits used in this analysis. The original signal is reconstructed very accurately by the decrypting circuit and Arduino. The original and deciphered binary signal is shown in Fig. 6.

From different grounds and power supplies, our circuit accurately sent and reconstructed a message with under a 1% error despite an offset voltage of 3V. Because of the chaotic "noise," coupled chaotic circuits have the potential to be a powerful encryption method.

III. FINAL WORDS

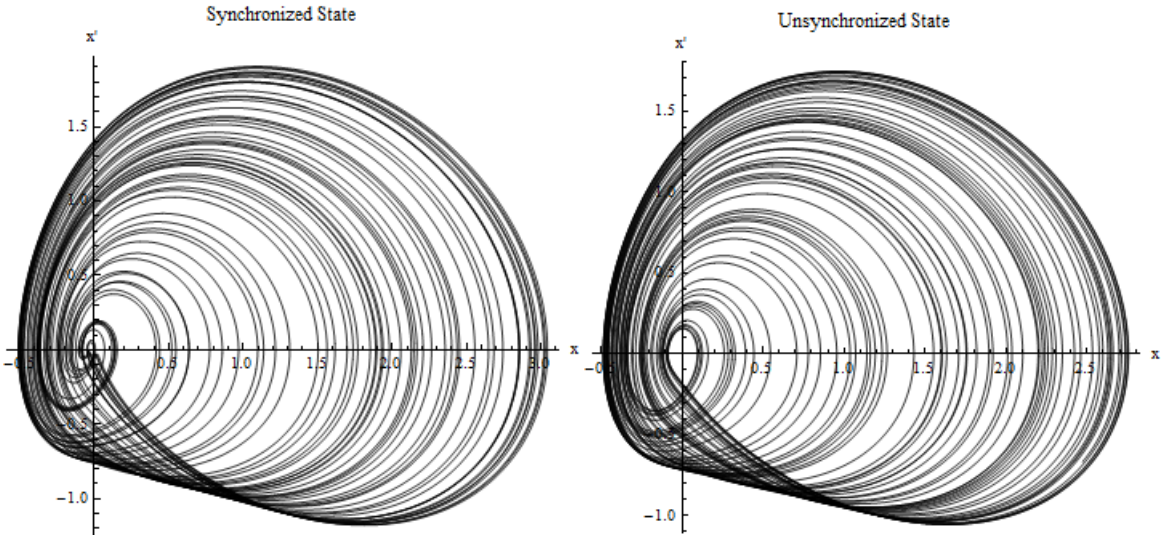
A. Extensions

The ability to send messages from different power supplies was a big step on the way to an effective circuit, but there is still much work to be done before our circuit could be used as a practical means for encrypted communication. Two criteria must be met for an effective encryption:

1. The phase portrait for the transmitting circuit cannot differ greatly between sending a zero and a one. If the phase portraits are distinct enough, one could recover the signal despite the chaotic noise.

2. The modes in which the binary signal is sent must fall within a chaotic regime.

Although it seems simple enough, in practice it can be difficult to get a reliable signal in a chaotic regime without differing the phase portrait greatly. Admittedly, we simply tried R_T values until



(a) (b)

FIG. 7: Phase portraits for a zero and one in binary code, respectively. There is only ∼.3V difference in both width and height between the two states.

we found an effective pair to create binary code. Much more research can be done on the most effective choices for R_T such that zeros and ones are distinguishable to the receiver, but not to others. The two modes used in our analysis are plotted side by side in Fig. 7.

Another area in which the circuit can improve is in its speed and accuracy. It took multiple minutes to send a few paragraphs of text. If the speed at which the message is sent is increased, the signal is not clear enough to decipher by the decrypting circuit. In today's society, this is not an effective means of communication despite the power of the encryption message.

A natural extension is the construction of a transmitter circuit that could send wireless messages to a receiver. The transmitter and receiver already operate on different grounds, with the only connection being the twisted pair. Thus it is not a farfetched idea to send the binary signal wirelessly between the circuits.

Throughout the scope of this research, we have assumed that hiding a binary signal amongst chaos is an effective encryption method. For a thorough analysis, we must test the validity of such a claim. If phase portraits or other representations of the data are unique, there may be ways to "work backwards" from intercepted data to recreate the circuit from the plot. If the representations of data are not unique, one could engineer a similar circuit that could decrypt the binary message without a deep knowledge of the original. Both possibilities could compromise the integrity of our method and should be examined.

B. Conclusions

Since its discovery in the 20^{th} century, chaos theory has fascinated people from all walks of life. One of its many applications is to the world of cryptography. We designed and build chaotic circuits based on [5] that can send and receive messages even when the transmitter and

receiver are connected to different power supplies. The transmitting and receiving circuit can synchronize and desynchronize their chaotic modes to send a binary code. Messages were sent with under a 1% decryption error but the limit of speed and reliability of the transmission have yet to be realized.

Chaotic circuits can provide a cheap and accurate glimpse of chaotic systems at an undergraduate level. Through the analysis, we have generated and used phase portraits, bifurcation points, nodal analysis and circuit design with great agreement between theory and experiment. Chaos theory bridges the predictable world of the physics laboratory with the seemingly random and disordered world associated with our everyday experience. Chaotic systems have only begun to show their usefulness and studying their properties will continue to give us a greater insight into the world in which we live.

Appendix A: Nodal Analysis

This appendix derives Eqs. (2)-(3). Components are labelled as in Fig. 1. Because each op-amp creates a virtual ground, our calculations are greatly simplified. Via the "golden rules" for op-amps, $0 = V_{11} = V_{13} = V_{15} = V_{17} = V_{19}$. Because there are no current sources, we apply

$$V_{\text{node}} \sum_j \frac{1}{R_j} = \sum_j \frac{V_{s_j}}{R_j} + \sum \frac{V_j}{R_j} \quad \text{(A1)}$$

at each node of interest. Following these steps, and letting $x = V_8$, we arrive at the node equations

$$\begin{aligned} V_1 &= -R_{20}C_6\dot{x}, \\ V_2 &= R_{16}R_{20}C_5C_6\ddot{x}, \\ V_3 &= -R_{15}\Big(\frac{V_0}{R_{00}} + \frac{V_2}{R_{14}} + \frac{V_2}{R_{13}+R_{v_2}} \\ &\qquad + C_4C_5C_6R_{16}R_{20}\dddot{x}\Big), \text{and} \\ V_3 &= -\frac{R_{17}}{R_{18}}V_1 - \frac{R_{17}}{R_{19}}D(x). \end{aligned} \quad \text{(A2)}$$

Solving this system of equations yields Eqs. (2)-(3).

Appendix B: Subcircuits

The circuit is split into five basic parts: the transmitter, the twisted pair, the decrypter, the coupler, and the receiver as seen in Figs. 8a, 8c, 8d, 8e, 8f, respectively. The transmitting circuit contains R_T, which is the subcircuit that generates the binary signal. R_T is shown in Fig. 8b. An arduino sends a binary message: 0V for a 0, and 5V for a 1. When a 0 is sent, the transistors act as an open. When a 1 is sent, the transistors act as a short. This changes the parameter R_T and effectively switches the receiving circuit between two chaotic modes.

The decrypting circuit is split into four parts. In part (a), x_1 and x_2 are sent to a differential amplifier, which takes their difference: $x_2 - x_1$. They then pass through (b), an ideal absolute value circuit. When the value of $x_2 - x_1$ is positive, the circuit acts as a unity buffer. When the value of $x_2 - x_1$ is negative, the circuit acts as an inverting amplifier. Part (c) is simply a low pass filter. Only low frequencies pass through, while the high frequencies are removed. Part (d) is the comparator. We first pick a threshold voltage V_{th}. If $x_2 - x_1$ is above V_{th}, it becomes amplified to 5V. If $x_2 - x_1$ is below V_{th}, it is suppressed to 0V. This creates

the binary signal that can be read by the Arduino.

The coupling circuit uses a differential amplifier to take the sum $.8x_1 + .2x_2$, which is then fed into the nonlinear subcircuit, $D(x)$, in the receiving circuit.

---

[1] N. I. Hall (Ed.) (1994), Exploring Chaos: A Guide to the New Science of Disorder (p. 7). W. W. Norton & Company, Inc.

[2] L.M. Pecora & T.L. Carroll, Physical Review Letters **64**, 821 (1990)

[3] S. Barnett, "The Encryption and Decryption of Digital Signals with Chaotic Circuits." Dated: 07/16/12

[4] T. Knighton, "Chaos and Analog Signal Encryption." Dated: 1/21/2012

[5] K. Kiers, D. Schmidt, & J.C. Sprott (2004), American Journal of Physics **72**, 1

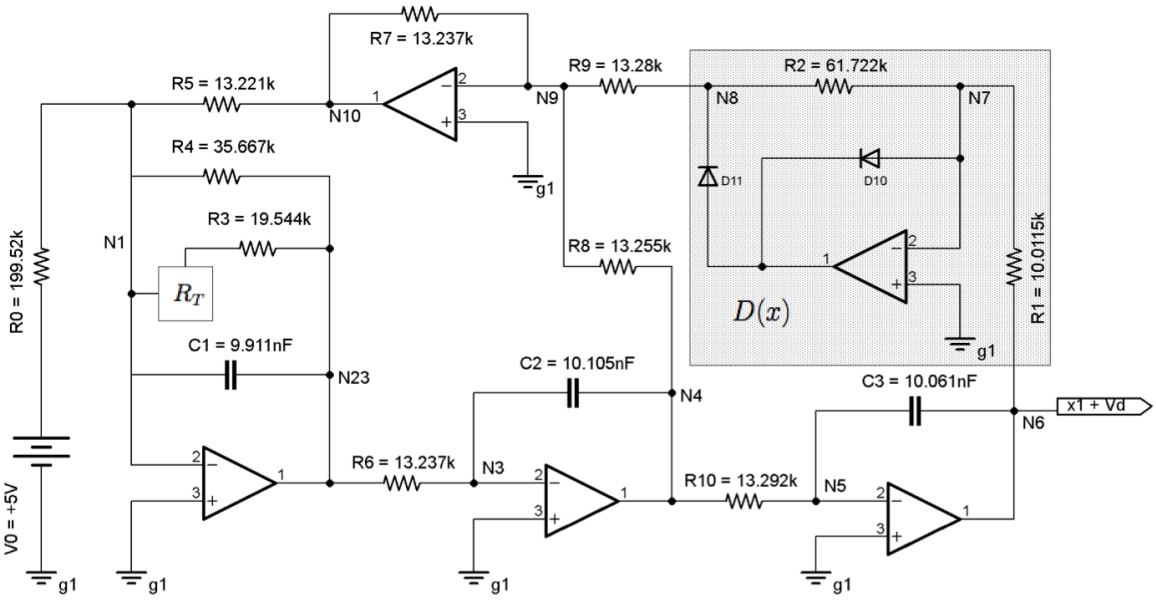


FIG. 8a: Transmitting Circuit

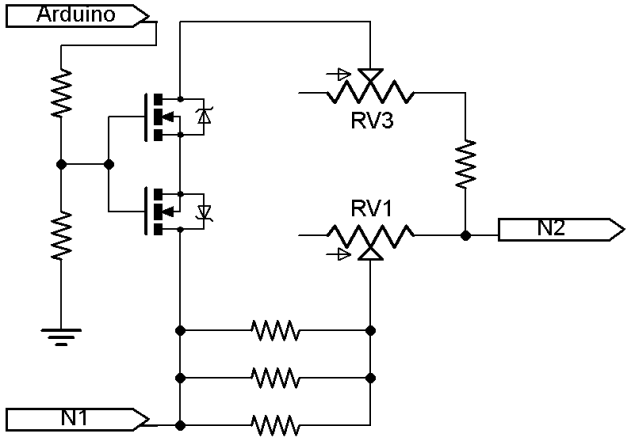


FIG. 8b: R_T subcircuit of Fig. 8a. The transistors act as a short when the Arduino sends a 5V signal but act as an open at 0V.

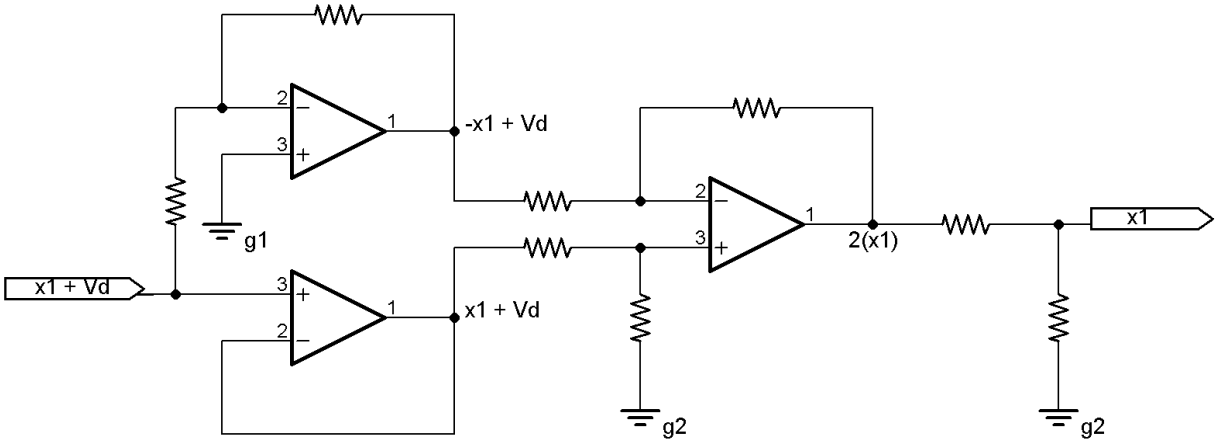


FIG. 8c: Subcircuit that generates a twisted pair. The twisted pair is then used to remove the reference to the transmitter circuit's ground, g_1.

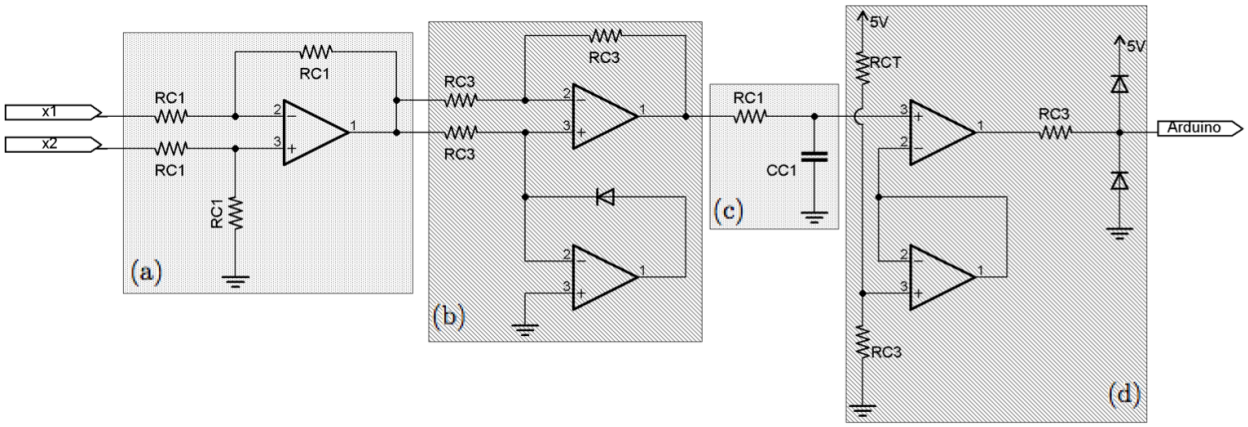


FIG. 8d: Decrypting Circuit. The function of the shaded subcircuits are explained in Appendix B. $R_{C1} = 100\text{k}\Omega$, $R_{C2} = 200\text{k}\Omega$, $R_{C3} = 10\text{k}\Omega$, and $C_{C1} = 10\mu\text{F}$.

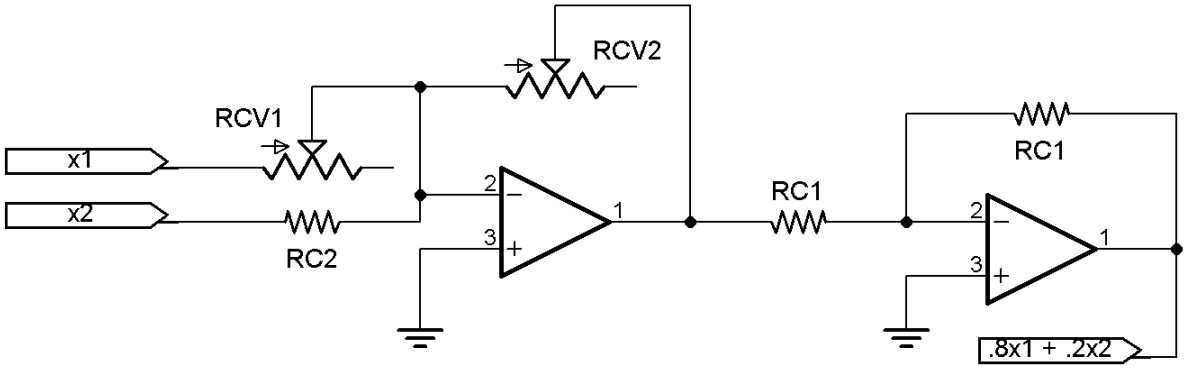


FIG. 8e: Coupling Circuit. Resistor values are defined as in Fig. 8d.

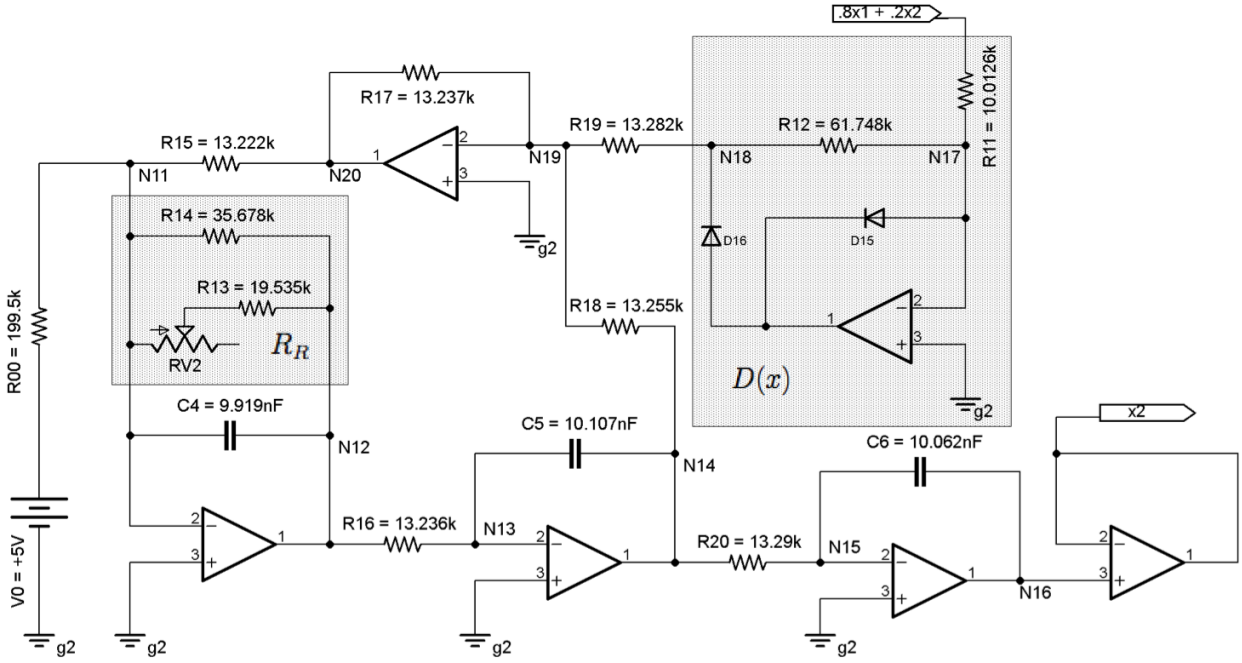


FIG. 8f: Receiving Circuit. Synchronizes with the receiving circuit in Fig. 8a.

FIG. 8: Final circuit used for our binary message analysis. Its functionality is explored in Sec. II B and analyzed more deeply in Appendix B.