Synchronization and Encryption with a Pair of Simple Chaotic Circuits

Ken Kiers
Physics and Engineering Department, Taylor University
236 West Reade Ave., Upland, IN 46989
knkiers@taylor.edu

Abstract

In recent years, students in Taylor University’s Physics Capstone Course have built pairs of nearly identical chaotic circuits that they have used to encrypt, and subsequently decrypt, a signal. These circuits can be constructed using inexpensive parts and can also be modeled very accurately using relatively simple differential equations. Students have found the construction and analysis of these systems to be technically challenging, yet, ultimately, very rewarding. Two methods of encryption have been studied to date; both methods will be demonstrated in this workshop. In the first approach, a digital potentiometer in one of the chaotic circuits is switched back and forth between two settings (corresponding to “ones” and “zeros”) in such a way that a binary data stream is encrypted within the chaotic output of the circuit. The other circuit is used to decrypt this data stream. In the second approach, a small analog signal is added to the chaotic output of the first circuit, and is then extracted by the second circuit. In both approaches, the decryption of the signal relies on the fact that the second circuit is able to synchronize its output to the output of the first circuit if the two circuits are identical to each other. Changing the value of one of the resistors in the first circuit (as in the first approach), or adding a spurious signal to its output (as in the second approach), causes the second circuit to be unable to synchronize with the first. In both cases, comparison of the output of the second circuit to that of the first allows for the recovery of the original signal.

1. Introduction

Two nearly identical chaotic circuits can be arranged in such a way that they synchronize with each other under certain conditions. In this arrangement, the first circuit (the “transmitter”) sends out a chaotic signal and the second (the “receiver”) synchronizes its output to that of the first. This arrangement of circuits can also be used to encrypt, and subsequently decrypt, a signal. (See, for example, Refs. [1, 2].) The essential point is that, if the circuits are nearly identical, the second circuit can synchronize with the first. However, if the first circuit is not identical to the second circuit, or if an analog signal is added to the output of the first circuit, then the second circuit will no longer be able to synchronize with the first. The first approach allows for the encryption of a binary data stream. The second allows for the encryption of an analog signal. In this workshop we demonstrate both processes using the circuit described in Ref. [3], but modified to run at a higher frequency.
1.1 Digital encryption

To encrypt a digital signal, an Arduino is used to control a digital potentiometer in the transmission circuit. One setting of the digital pot is such that the two circuits are nearly identical, so that they synchronize. The other setting of the digital potentiometer is such that the circuits are no longer identical, in which case the receiver circuit fails to synchronize with the transmitter. Figure 1 shows a block diagram representing this arrangement.

Note that, in our implementation, the circuit must be floated at a false ground, since the digital potentiometers always need to be between 0 and 5 V. Some further discussion of this point may be found below. (There are most likely digital potentiometers that are not subject to this constraint.)

1.2 Analog encryption

To encrypt an analog signal, two “identical” chaotic circuits are constructed and coupled as above. Then a small analog signal is added to the output of the first circuit, as indicated in Fig. 2. The difference $x_1 + \sigma - x_2$ (see the figure) yields a slightly noisy approximation to $\sigma$. In the workshop, we take $\sigma$ to be a sine wave with amplitude 10 mV and frequency 200 Hz. We also consider the case in which $\sigma$ (the signal to be encrypted) is taken from an audio file.

2. Hand-outs and files

The hand-outs and files listed below are available as part of this workshop. Some of these are available from the conference website; others directly from the presenter (please see above for contact information).


2. Assignment #1, Physics Senior Capstone (PHY493), Interterm, 2012. Available from presenter.


4. Using a Digital Potentiometer with the Arduino.

5. “Chaos and Analog Signal Encryption,” Talbot Knighton, 1/21/2012. (Small modifications have been made to the paper by KK. Please note that the circuit diagram in Fig. 1 contains two mistakes. These are corrected by hand on the hand-out.) Zooming in on Fig. 1 in the electronic version of this paper allows for the identification of specific component values.


7. “Synchronization and Encryption with a Pair of Simple Chaotic Circuits,” Ken Kiers, PowerPoint presentation.
Figure 1: Block diagram showing the configuration used for digital encryption. The digital potentiometer has two settings, which are controlled by the Arduino. At one setting, the transmitter and receiver circuits are “identical” (or close to it), and $x_2$ synchronizes with $x_1$. At the other setting, $x_2$ fails to synchronize. One of these settings corresponds to a “zero” and the other to a “one,” allowing for the transmission and reception of a binary data stream. Note that, in practice, $x_2$ and $x_1$ differ for both settings of the digital potentiometer. The difference is larger in one case than in the other, however. For further details, see the paper by Steven Barnett (available at the BFY website).
Figure 2: Block diagram showing the configuration used for analog encryption. In this case, taking the difference of $x_1 + \sigma$ and $x_2$ yields an approximation of $\sigma$, thus decrypting the signal. Further details may be found in the paper by Tal Knighton (available at the BFY website).


3. Supplies and some helpful hints

The following supplies are needed to construct the circuits described in this workshop:

1. Solderless breadboard(s).
2. Approximately 15 operational amplifiers (five per chaotic circuit; up to five additional ones for mixing, etc.) We used MC33078P chips, which have two op amps on each chip.

3. Resistors (see students’ papers for details). Note that it is best to get 1% resistors; the transmitter and receiver circuits need to be as similar as possible.

4. Analog potentiometers (useful for fine-tuning some of the resistance values).

5. Capacitors for the integrating op amps (see students’ papers for details). Again, it is helpful to purchase capacitors with smaller tolerance values.

6. By-pass capacitors for the positive and negative rails for each op amp chip. These are important to mitigate noise in the circuits.

7. Four diodes (two for each circuit). We use 1N4148 diodes.

8. Voltage regulator. This is useful for supplying a stable DC input voltage. The voltage regulator may require some capacitors, as well.

9. Digital oscilloscope, power supplies, function generator (for analog encryption).

10. Arduino (for digital encryption).

11. Digital potentiometer(s) (for digital encryption). We use the DS1803-050, which has two digital potentiometers on one chip. Note that the low and wiper leads both need to be between 0 and 5 V for this chip, so the circuit need to be “floated” at a false ground to accommodate the digital pots.

Some helpful hints:

1. The following link contains some helpful hints on working with solderless breadboards. It was put together by Dr. Joel Gegner of Taylor University. 
   https://sites.google.com/site/enp33111/labs/bread?pageMoved=labs.

2. Before doing anything else, sort resistors and capacitors into “matching” pairs. That is, find pairs of resistors that have very (very, very) close resistances, and the same for the capacitors. One resistor from a pair can be used in one circuit, and the other can be used in the exact same location in the other circuit. In this manner, nearly identical circuits can be constructed. Students often ask, “How close is close enough?” My usual answer is, “The closer you can get them, the better.” Another possible response is to encourage the students to simulate the synchronization by solving the differential equations numerically in Mathematica (using actual component values rather than ideal ones). Then they will be able to “experiment” with component values to see how close they need to be in order achieve a desired level of synchronization.

3. Try building one circuit first. Once that circuit is running, build the second. Then try to couple them together to achieve synchronization. It is apparently quite important that the “0.8” and the “0.2” in the summing circuit sum up to exactly “1”.

5
4. When building the individual chaotic circuits, it is important to include by-pass capacitors (between the positive rail and ground, and between the negative rail and ground) for each of the op amp chips. These by-pass caps help to reduce noise in the circuit. They are not shown in any of the circuit diagrams, but it is important to include them.

5. Once synchronization has been achieved, an analog signal can be added (see Tal Knighton's paper). This can be done using a function generator. Alternatively, music can be sampled from a laptop using the output from the headphone jack.

6. For the digital encryption case (see Steven Barnett’s paper), note that the digital pots that we used require the “low” and “wiper” pins to both be between 0 and 5 V. This means that the entire circuit needs to be “floated” at a false ground. The “false ground” can be obtained by using a regulator and voltage divider, followed by a unity gain buffer op amp arrangement. The “grounds” of each of the op amps in the rest of the circuit would then be referenced to this false ground.

7. The appendices in the students’ papers are helpful starting points for deriving the differential equations corresponding to the circuits. We use the “node analysis” approach.

4. Concluding remarks

The chaotic circuit employed as the essential building block in this workshop has been studied over the course of several years by students at Taylor University. Construction and analysis of this circuit has provided a helpful review of (or, introduction to, in some cases) electronics, differential equations and numerical computation (using Mathematica, for example) and has provided students with a good introduction to the field of chaos and nonlinear dynamics. In the past, we have performed an in-depth analysis of the level of agreement between theory and experiment for this circuit [3]. We have also built and sold an undergraduate laboratory device based upon it (the “Electronic Chaos System,” formerly available through PASCO). More recently, engineering students at Taylor have constructed a new and improved “black box” lab device based on this circuit (demonstrated as part of the workshop).

During the past several years we have turned our attention to using pairs of these circuits as encryption/decryption devices. The work described in this workshop represents where we currently are on this project. There are certainly many ways in which the work could be improved or extended. The presenter would welcome future collaboration on this topic if the opportunity should arise.

References
