Chaotic Circuits and Encryption

Brad Aimone
Stephen Larson
June 16, 2006
Neurophysics Lab

Introduction

Chaotic dynamics are a behavior exhibited by some nonlinear dynamical systems. Despite an appearance of randomness, chaotic dynamics are in fact deterministic. The appearance of randomness is caused by a high dependence on initial conditions exhibited in chaotic regimes. The visual appearance of these dynamics, when plotted against the oscillating input voltage, is of a system whose state "hovers" around a limit-cycle, but whose state never quite passes through the same trajectory twice. Consequently, plots of chaotic dynamics generally display a thick band of activity indicating the multiple trajectories through phase space, rather than a thin line that would suggest a single stable trajectory.

Chaotic dynamics in electronic systems have been a subject of interest since Linsay's seminal paper in 1981 that demonstrated a simple RLD circuit was capable of producing them.
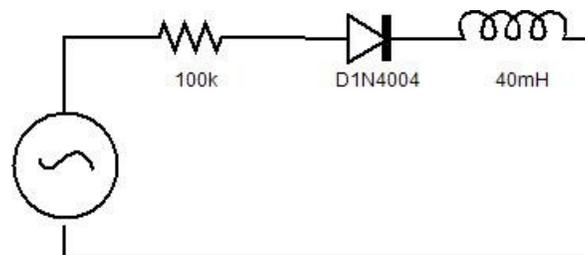
Figure 1: A simple RLD circuit capable of producing chaotic dynamics

The voltage measured at a point between the resistor and the diode will exhibit chaotic dynamics when the voltage source provides an oscillatory input at the resonant frequency of the circuit.

Chaotic Synchronization Demonstrated

In 1993, Newell et al. reported the synchronization of two separate chaotic circuits. These results were confirmed and methodology improved on by Mozdy et al in 1995. The basic idea that was employed to accomplish this was that of occasional Proportional Feedback. Essentially the idea is that if two systems are relatively similar to begin with, only small (linear) corrections will be needed in order to match one to the other. As a result, what is needed is circuitry to compare the master signal to the slave signal and circuitry to add that difference into the slave signal.

Chaotic Synchronization Opens Door to Chaotic Encryption

The ability to synchronize chaotic circuits opened the door for using the unpredictable nature of chaotic dynamics as a way to encrypt signals along a communication channel.

Neff and Carroll described this in 1993, and it was revisited by Wang et al in 2004. The idea is as follows: A sender encrypts an information signal using a chaotic carrier. The intercepted transmission is chaotic and thus undecipherable. The receiver removes chaotic signal from transmitted signal, revealing the information signal. Ideally, without chaotic parameters and equations (for example, initial conditions), chaos cannot be separated from signal.

Interested to explore the results reported in the afore-mentioned references, we set about to implement a circuit that exhibited chaotic dynamics, chaotic synchronization, and chaotic encryption.

Results

Chaos in RLD circuit

The voltage recorded from the wire between the resistor and the diode in the RDL circuit setup that we built. For studies which looked only at the behavior of the chaotic circuit, the input voltage was monitored as well as a reference for the chaos. In this example, the signal output was in fact chaotic.
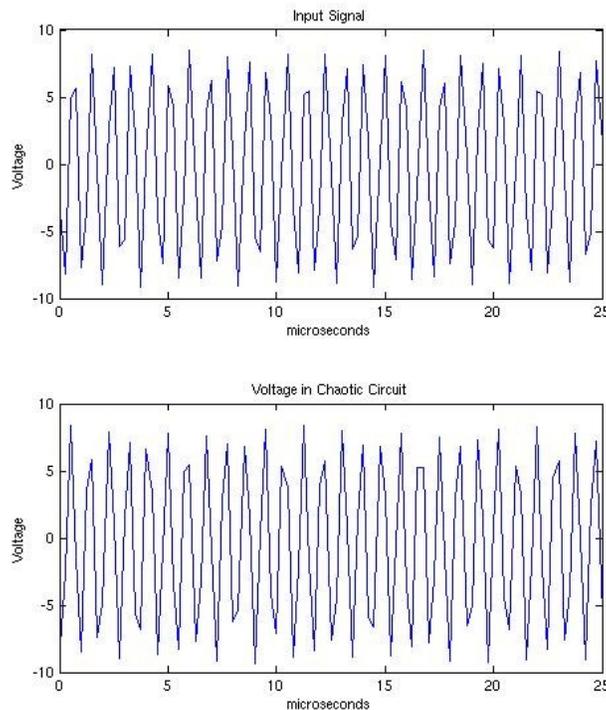
Figure 2: Trace of input signal (top) and chaotic signal (bottom)
at 121 kHz

Because chaotic behavior is not always immediately evident from a signal trace, especially one that is sampled at 4x the underlying oscillation as is here, other visualization techniques must be used to observe the chaos. By plotting V_{Input} vs V_{RD} we

are in essence plotting two 'states' of the system. In a non-chaotic oscillating system, the relationship of V_{Input} and V_{RD} is a limit cycle – if V_{Input} is known, the V_{RD} is known to be one or several values. However, during chaotic behavior, V_{RD} is not predictable knowing V_{Input} alone, but also requires a full knowledge of the other states. During chaotic behavior, the system does not repeat the exact state twice - doing so in a dynamical system would result in following the previously taken path. Therefore, while the (V_{input}, V_{RD}) relationship may have previously been encountered, some other unmeasured state variable must be different, and the previously taken path is not the same. Therefore, the two paths can cross without interference. As a result, the chaotic system does not follow a limit cycle but rather forms a 'cloud' of data points around the limit cycle. Figure 2 shows an example of a V_{input}, V_{RD} plot for a non-chaotic system and a chaotic system.
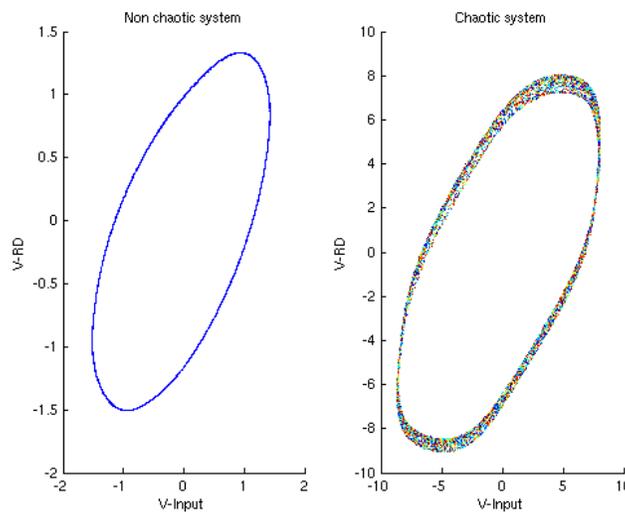
Figure 3: Phase space plot of non-chaotic signal (left) and chaotic signal (right). Plotted is the relationship between the input voltage (x-axis) and V_{RD} (y-axis).

Although we are only recording two 'dimensions' of the chaotic system, the system itself must exist in greater than two dimensions to allow this overlapping behavior in 2-d space. Ideally we would be able to plot more than two state variables simultaneously. Despite the fact that we are only recording two channels, because the behavior of V_{RD} is in fact a deterministic function of N unseen variables, plotting V_{RD} at distinct time steps can capture the relationship of these variables. Therefore, $V_{RD}(t+1)$ is a separate 'state' than $V_{RD}(t)$. Figure 3 shows this time delay approach to plotting
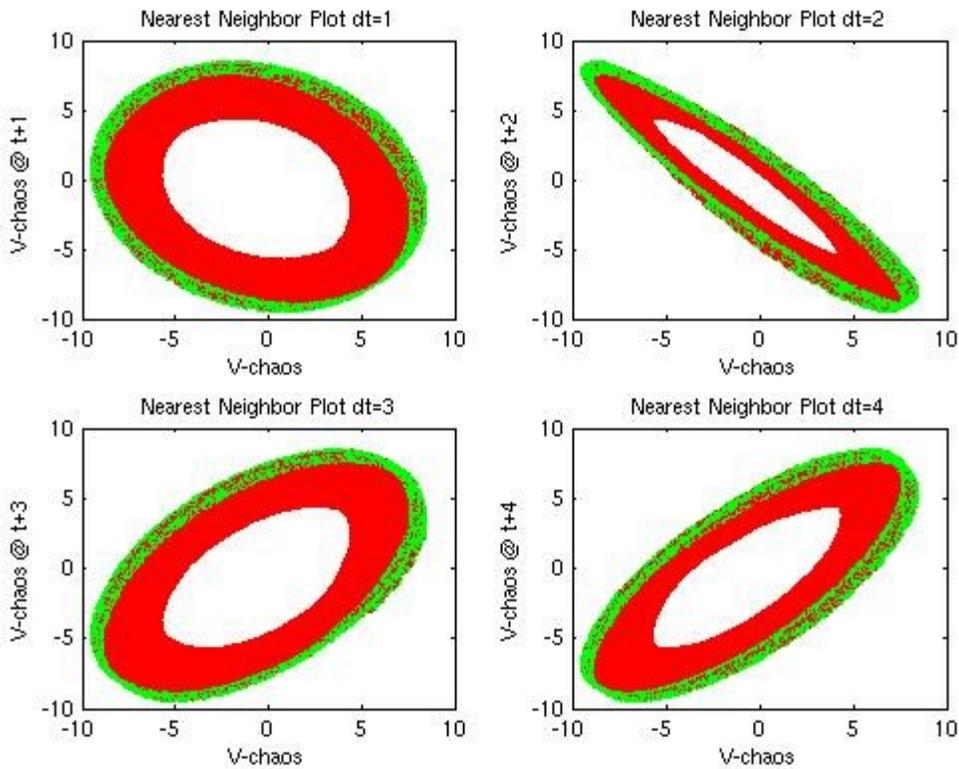
Figure 4: Time delay plot of chaotic signal. For each x-coordinate, the green dot at the y-coordinate represents the V_{RD} at a following time (dt=1,2,3 or 4). Red lines were drawn between consecutive data points to show associations between points at t and t+dt. 10000 data points are shown here.

Summary of chaos results

Chaotic behavior does not simply appear at the chaotic frequency (121kHz – the resonant frequency of the diode and the 10mH inductor). Rather, this chaotic behavior is highly dependent on the amplitude of oscillatory input. As the amplitude of the input into the system increases, the system proceeds through several 'bifurcation' stages that are . This is immediately evident from the V_{Input}, V_{RD} plots shown in Figure 4 – as amplitude increases, the limit cycle splits into two cycles which cross one another. This indicates that the system is now in a limit cycle moving through 3 dimensions, not just two. Increasing the amplitude will continue to increase these bifurcations – or simply an increase in the complexity of the limit cycle – until the system becomes chaotic.
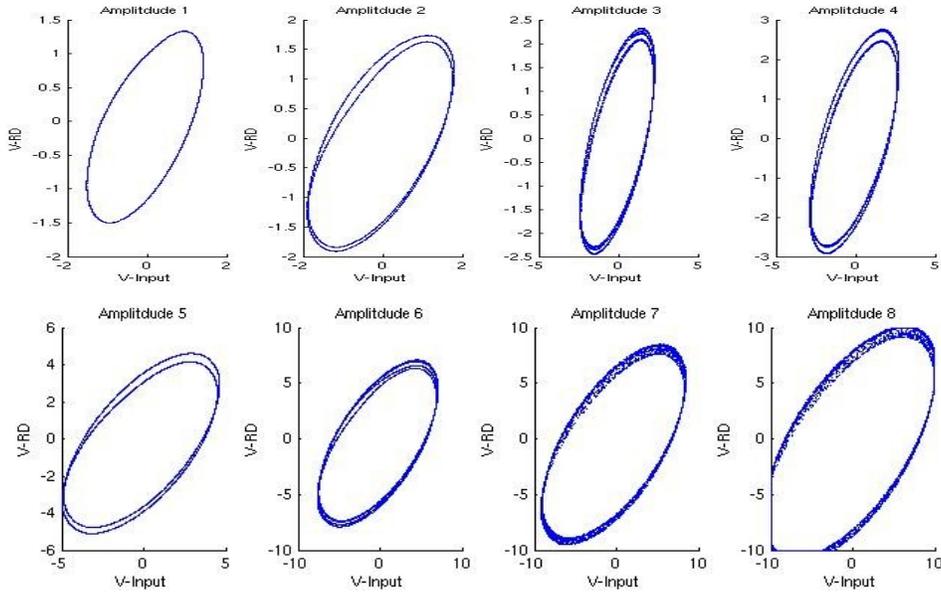
Figure 5: Phase space plot (V_{Input} vs V_{RD}) of circuit at chaotic frequency with increasing amplitude. Note how a simple limit cycle exists at low amplitude but raising amplitude (towards the right) causes bifurcations and ultimately chaos.

Summary of Synchronization Results

We analyzed the synchronization of our two chaotic circuits in a similar manner to a single chaotic circuit described above. However, rather than expecting to see a chaotic relationship between V_{Chaos1} and V_{Chaos2}, we had hoped to see a linear relationship ($V_{Chaos1}=V_{Chaos2}$ for all points), or at the very least a limit cycle suggesting that the two variables are related but offset in phase space.
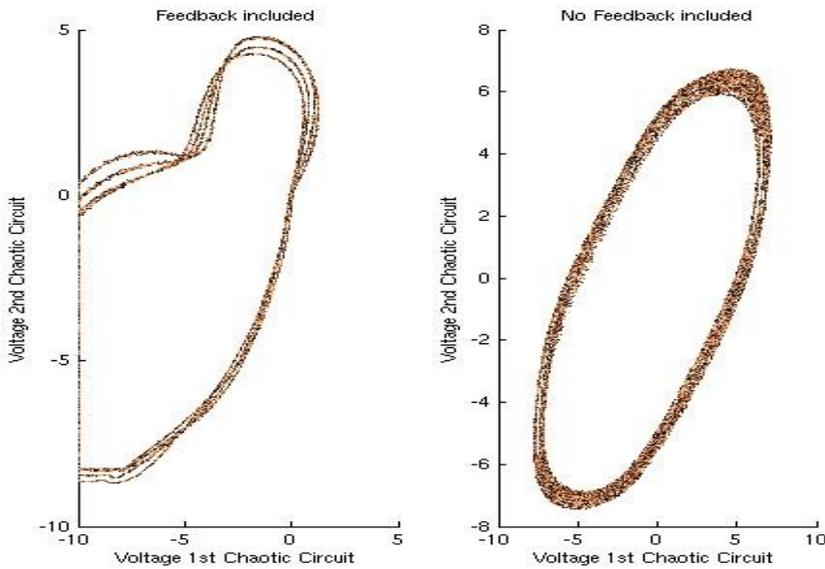
Figure 6: Scatter plot of dual chaotic circuits, $V_{RD}1$ vs $V_{RD}2$. Left is plot of when 2nd chaotic circuit had correction feedback and right is plot without feedback.

Encryption

Although we did not have success in synchronizing the circuits, we nonetheless sought to encrypt information within our chaotic circuit. Our approach was to use a carrier wave of the same frequency as the chaotic signal, and then embed a signal within that carrier wave via amplitude modulation (AM). Presumably, adding this AM-carrier signal to the chaotic signal would then require decryption with the same chaotic signal to read out.

The following graphs illustrate an example of our attempt to encrypt information into the chaotic signal. In each instance, we plot a spectrogram of the signal – the Fourier spectrum of discrete time frames of the signal and how that changes over time.
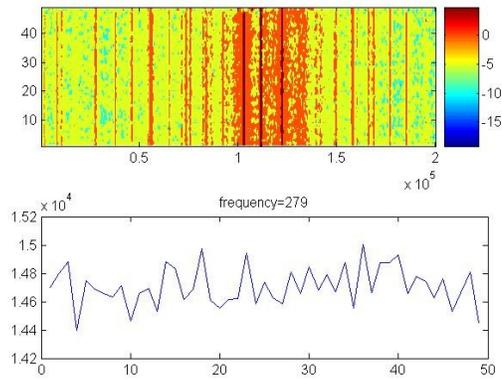
Figure 7: Temporal spectrogram of chaotic frequencies. X-axis is frequency, y-axis is time. Bottom plot represents temporal dynamics of the frequency with the highest power. This plot represents the spectrogram of a chaotic signal.
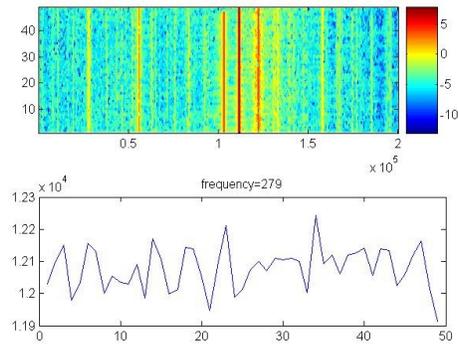
Figure 8: Same as above, this plot represents the spectrogram of a chaotic signal with embedded 'carrier signal'
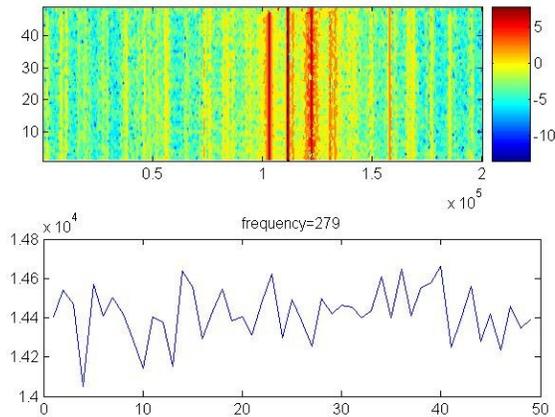
Figure 9: Same as above, this plot represents the spectrogram of a chaotic signal with the carrier signal minus the chaotic signal (no time delay)

Discussion

Our results demonstrate that chaotic dynamics are achievable in a simple RLD circuit, confirming Linsay's basic result. Our observation was that the chaotic regime of our circuit was amplitude dependent. As the amplitude of a particular input frequency was increased, we observed a progression of dynamical regimes that began with oscillatory behavior that was not chaotic, continued through bifurcations in the oscillation, and ended in chaotic oscillations.

We were not able to reproduce results of Mozdy et al. to observe synchronization between two RLD circuits exhibiting chaotic dynamics. However, this result is very similar to that reported by Richert and Whitmer. They observed, as we did, that "using the circuit as described, synchronization was only possible in non-chaotic regimes" [data not included]. We observed a trade off between synchronization and chaotic oscillation between the two circuits. Several explanations for this behavior can be inferred, which center around the explanation, also reached by Richert and Whitmer, that the unidirectional control circuit was working incorrectly.

One explanation is that our chaotic oscillations were at 121kHz, and by the time that our circuit calculates the necessary correction, the slave oscillator is already beyond the point where the correction would have the desired effect. While possibly having the desired effect if instantaneous, the simple linear correction approach to synchrony is probably not effective because of the time delays in the op-amps and transmission. Despite attempting to solve the problem with a delay circuit, we did not seem to be able to compensate for this effect. Richert and Whitmer suggested that "op amps with a higher gain than the TL071CN" might help to reduce the lag.

Another explanation centers the problem on the inductors... we were not able to use inductors of the appropriate size called for in the design (100mH). Consequently we attempted to compensate for this in the design. One of the strange effects that was observed that may have been a consequence of this was that the chaotic dynamics of the master circuit would drift out of a chaotic regime into a non-chaotic one. This effect could be reset by touching the inductor in the circuit, but the drift would start over from the beginning. We addressed this by increasing the size of the capacitor in our variable gain filter unit, and this seemed to fix the problem. This example however demonstrated that without a thorough parameter tuning of the system, attempts to get synchrony working would be difficult since we did not have a principled way to address issues like this.

Our ability to fully build a chaotic encryption system was hampered by our lack of a system that appropriately synchronized. Despite this, we got a result that demonstrates the ability to perform a simple encryption using the pseudo-random nature of chaotic dynamics. It remains to be seen the degree to which a synchronized slave circuit could decrypt a signal in the manner that we encrypted.

Methods

Initial investigations of chaotic dynamics were conducted on a breadboard with the simple design displayed in Figure 1. We discovered that identifying the chaotic regime of the circuit could be done by conducting parameter sweeps of frequency and amplitude of the input oscillatory voltage signal. By plotting input voltage against output voltage, we were able to visually identify chaotic regimes by observing patterns that exhibited thick trajectory bands.
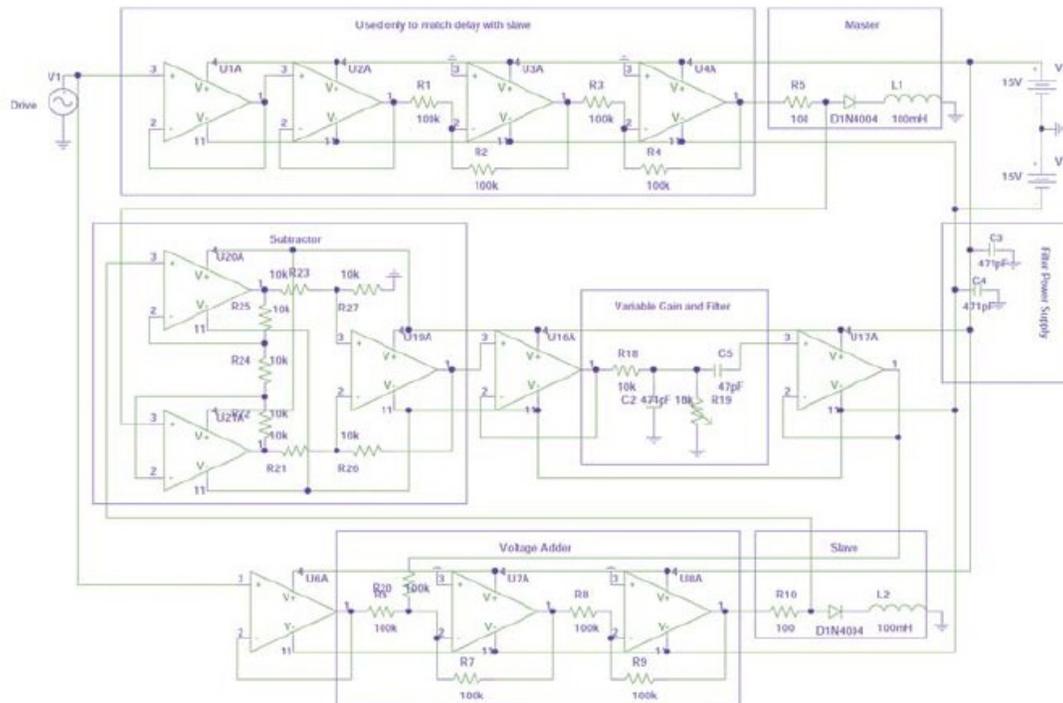
Figure 10: Circuit diagram from Richert and Whitmer, 2003. The two chaotic circuits are labeled as Master and Slave

We relied heavily on the circuit design of Richert and Whitmer, 2003, when exploring chaotic synchronization. As mentioned in the introduction, this circuit uses the notion of Occasional Proportional Feedback to achieve synchrony. To generate the correction signal, the states of the two circuits are compared, and a scaled down version of this difference is added to the slave's drive signal. This correction signal can be thought of as a negative feedback signal, or weak coupling in a coupled oscillator system. The coupling is unidirectional, which means that the master circuit does not have any correction or feedback applied to its drive.

All op amps are ST's TL071CN.

The following sections go into more detail about each part of the circuit.

Subtracter and Variable Gain Circuit
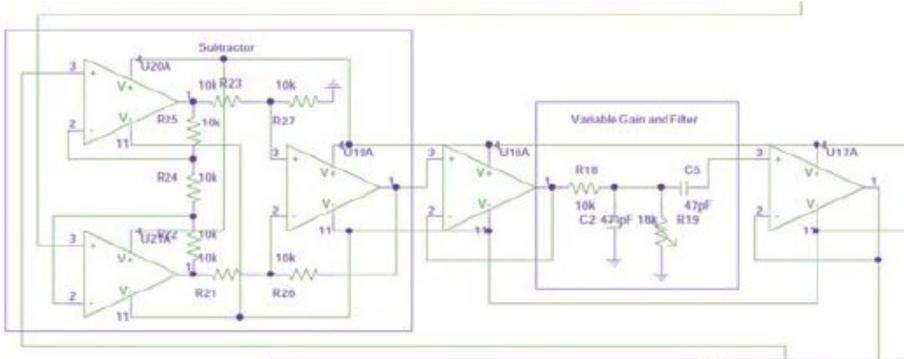
Figure 11: Richert and Whitmer's Subtracter Circuit

The subtracter unit, responsible for measuring the difference between the slave and the master signals, works in the following way. It is comprised of three op amps. Two op amps act as buffers and the third computes the subtraction. This subtracted voltage is then scaled down to produce a variable gain before being fed back into the slave. This is accomplished by a simple RC filter circuit using a variable resistor to adjust the tuning of the filter.

Voltage Adder Circuit
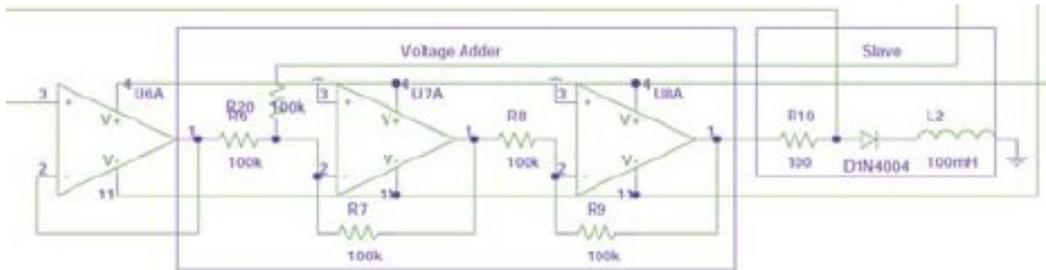
Figure 12: Richert and Whitmer's Voltage Adder Circuit plus Slave chaotic oscillator

The voltage adder circuit is based on a two op amp circuit that adds current. A consequence of this is that voltage is inverted, therefore, to correct for this, a third op amp operates as an inverter.

Delay Circuit
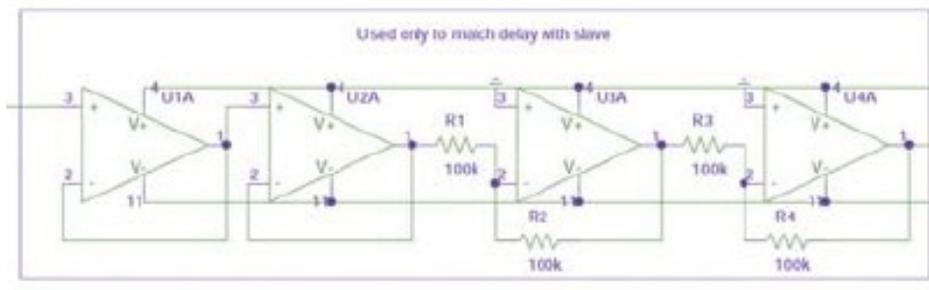
Figure 13: Richert and Whitmer's Delay Circuit

A delay circuit is also included. Phase lag introduced by the op amps is significant, thus this portion of the circuit is intended to compensate for that. Op amps between the drive signal and the master oscillator match the amount of delay between the drive and the slave oscillator.

Encryption

For the simple encryption circuit we built a second adder circuit as described above and used it to add a second oscillatory signal from a separate signal generator to the chaotic carrier coming from the master chaotic circuit.

Recording and Analysis

Data was recorded using a National Instruments signal acquisition card, sampled at a rate of 400 kHz, and uploaded into a custom designed Labview program which permitted us to monitor signal acquisition and exported the signal data to a text file. The signal data was then uploaded into MATLAB for further analysis.

Acknowledgments

References

Linsay, P.S. (1981). Period doubling and chaotic behavior in a driven anharmonic
oscillator. Physical Review Letters, 19, 1349-1352.
Mozdy, E., Newell, T.C., Alsing, P.M., Kovanis, V., Gavrielides, A. (1995).
Synchronization and control in a unidirectionally coupled array of chaotic diode resonators.
Physical Review E., 51(6), 5371-5376.
Neff & Carroll, Circuits That Get Chaos in Sync, Scientific American, August 1993
Newell, T.C., Alsing, P.M., Gavrielides, A., Kovanis, V., Synchronization of chaos using
proportional feedback. Physical Review E., 49(1), 313-318.
Richert, M., Whitmer, D., Chaotic Dynamics of RLD Oscillator, Unpublished lab report for biophysical
measurements lab, UCSD Physics Department, June 13, 2003.
Wang, X., Zhan, M., Lai, C.H., Gang, H., Error function attack of chaos synchronization based encryption
schemes, Chaos, 14(1), March 2004