# Multiple Channel Secure Communication Using Chaotic System Encoding

S. L. Miller
Sandia National Laboratories
Mail Stop 1080
P.O. Box 5800
Albuquerque, NM 87185-1080



Abstract

A new method to encrypt signals using chaotic systems has been developed that offers benefits over conventional chaotic encryption methods. The method simultaneously encodes multiple plaintext streams using a chaotic system; a key is required to extract the plaintext from the chaotic ciphertext. A working prototype demonstrates feasibility of the method by simultaneously encoding and decoding multiple audio signals using electrical circuits.

## 1. Introduction

Secure alternatives to conventional methods of communicating information are desperately needed. Chaotic dynamical systems exhibit properties that may be relevant to meeting this need. Chaotic signals have a broadband power spectrum, and it is not possible to predict their long term behavior either forward or backward in time. These and other properties of chaotic systems have been applied to achieve novel methods of encoding and decoding information [1-4].

Cryptanalysis has been performed [5] on a method of chaotic encryption that makes use of a property called synchronization. Chaotic synchronization is in fact one of the more extensively studied methods of chaotic encryption [see, for example refs. 6-9]. In the method analyzed, a small amplitude plaintext signal is masked by a large amplitude signal originating from a low dimensional chaotic system. The receiver, which extracts the plaintext from the chaotic ciphertext, is comprised of a dynamical system that physically synchronizes with the original encoding system. To properly synchronize, several criteria must be met. For example, the largest Lyapunov exponent of the receiving system must be negative (i.e. the receiver must be a stable system), and the modulated parameter must be small in amplitude compared to other oscillations in the system. Successful cryptanalysis has been demonstrated for synchronized systems when the following additional conditions are assumed: the chaotic encoder is of low dimensionality, the plaintext is small amplitude, an underlying attractor exists, and the form of the equations defining the chaotic system are known.

In this paper we present a new method to encrypt information using chaotic systems [10]. The properties and conditions that enable cryptanalysis of synchronized chaotic systems do not apply to this method. In addition to offering potential security benefits over existing chaotic encryption techniques, the present method exhibits an extremely diverse range of useful attributes and implementation methods.

## 2. General Method

The general method to encrypt information is to modulate the underlying dynamics of an n-dimensional chaotic system with one or more plaintext streams $S_i(t)$, as shown schematically in Fig. 1a. The state vector components of the chaotic system comprise the ciphertext $C_i(t)$. The encryption key is comprised of the specification of the chaotic system. This specification may take the form of 1) numerical parameters $p_j(t)$ for a mathematical specification of a numerically implemented chaotic system, or 2) values of parameters $p_j(t)$ for a physical specification of a physically implemented chaotic system. To decode the plaintext (Fig. 1b), the encoding process is simply reversed, i.e. the plaintext is *directly* decoded from the ciphertext, in contrast with the synchronization technique.

This type of complex high-dimensionality encryption system can be implemented not only in software, but as real physical systems, such as optical, electrical, magnetic, or electromechanical systems [11]. We defer discussion of the unique properties and benefits of the new method until Section 4. First, we illustrate a physical implementation of the method that uses a simple electrical circuit.

## 3. Implementation Example

Consider the simple circuit illustrated schematically in Fig. 2. This circuit contains conventional resistors, capacitors, analog multipliers, and operational amplifiers. The circuit spontaneously oscillates chaotically when the values of the physical components are within appropriate ranges. The time-varying state vector of this circuit can be described by the three components of ciphertext: $C_1(t)=x(t)$, $C_2(t)=y(t)$, and $C_{n=3}(t)=z(t)$. The dynamical behavior of this circuit is determined by the values of the circuit elements, and the signals $S_1(t)$, $S_2(t)$, and $S_3(t)$. The values of the circuit components comprise the key of the encoding system. The signals $S_1(t)$, $S_2(t)$, and $S_3(t)$

# DISCLAIMER

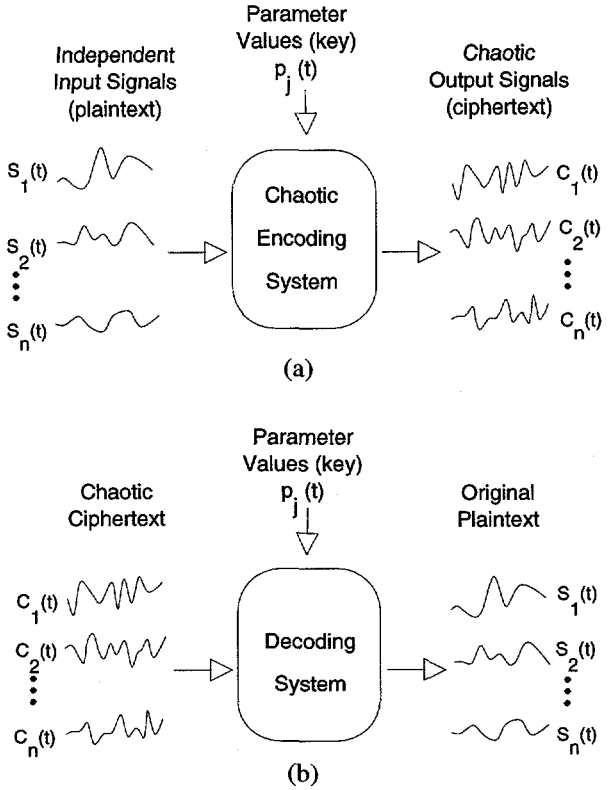


**Figure 1.** a) chaotic encoder simultaneously converts multiple streams of plaintext into a series of chaotic signals; b) plaintext is recovered by directly decoding the ciphertext

comprise three independent plaintext signals that are encoded by the system.

To simplify the example, the circuit shown in Fig. 2 was assembled using values of circuit components such that it may be approximated mathematically by

$$\begin{aligned} k\frac{dx}{dt} &= yz - S_1(t) \\ k\frac{dy}{dt} &= S_2(t)x - y - 5 \\ k\frac{dz}{dt} &= S_3(t) - (x-5)y \end{aligned} \qquad (1)$$

where $k$ is a time constant determined by the capacitor and certain resistor values.

The physical circuit was operated with plaintext $S_1(t)$ being a speech signal, and plaintext $S_2(t)$ and $S_3(t)$ being audio signals from two different radio stations. Figure 3 shows a brief portion of the signal $S_1(t)$. Figure 4 shows the cipher text resulting from the simultaneous encryption of the signal shown in Fig. 3 and the two radio stations.

To decode the plaintext from the ciphertext, circuits were constructed (Fig. 5) that invert the function of the encoding circuit. For the circuit elements chosen, these circuits can be mathematically approximated by

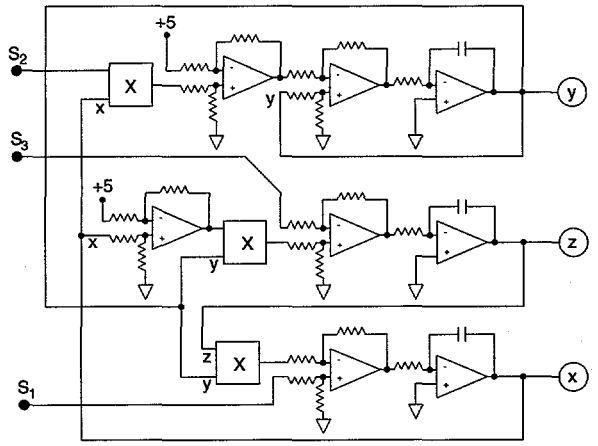


**Figure 2.** Chaotic encoding system comprised of an electrical circuit. This system simultaneously encodes three independent plaintext streams. The content of each of the three plaintext streams is dispersed between multiple ciphertext streams.

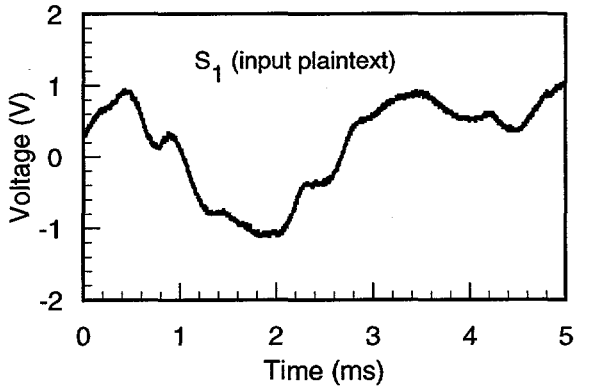


**Figure 3.** Plaintext comprising an audio signal from a microphone. This signal is one of three independent plaintext streams.

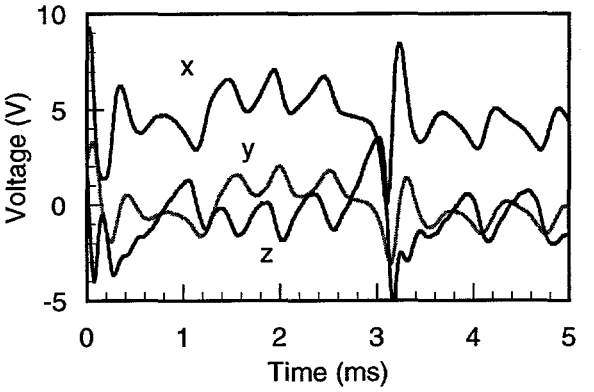


**Figure 4.** Ciphertext resulting from encoding three independent input signals, one of which is shown in Fig. 2.

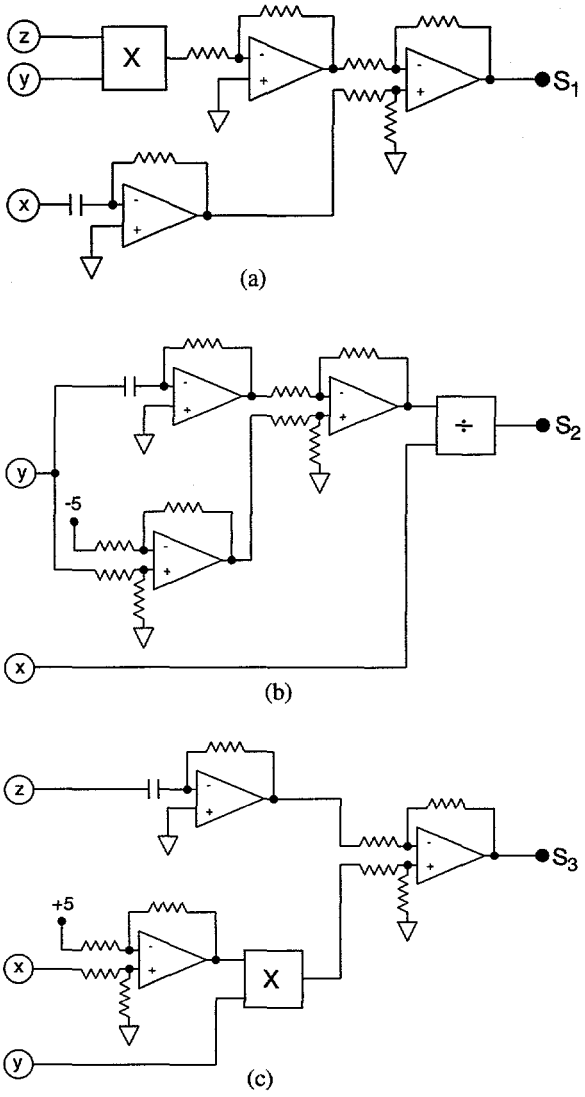


**Figure 5.** The circuits that decode the three plaintext streams $S_1(t)$, $S_2(t)$, and $S_3(t)$ from the ciphertext x(t), y(t) and z(t).

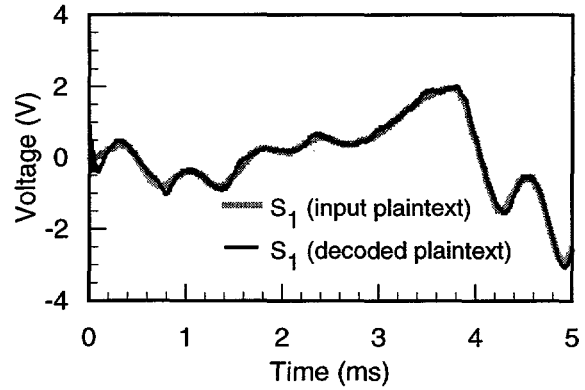


**Figure 6.** Comparison of original and decoded plaintext shows minimal distortion resulting from the encoding/transmission/decoding process.

$$S_1(t) = yz - k\frac{dx}{dt}$$
$$S_2(t) = \frac{k\frac{dy}{dt} + y + 5}{x} \qquad (2)$$
$$S_3(t) = k\frac{dz}{dt} + (x-5)y$$

In order for the plaintext to be decoded properly, the values of the circuit parameters, e.g. capacitors and resistors, must appropriately match those of the encoding circuit. Figure 6 shows audio plaintext $S_1(t)$, and the resulting plaintext after being encoded and decoded by the physical circuits described above. The close agreement is an indication that the encoding and decoding circuit parameters (the key) are closely, but not precisely, matched. The more complex the circuit, the more closely matched the circuit elements must be in order to accurately decode the plaintext.

We have thus demonstrated with a real circuit (although a very simple one) the basic concepts of the general method. We now discuss a number of very useful attributes of this type of encryption method.

## 4. Unique and Useful Attributes

*Encoding and decoding rate may be very fast.* This is because encoding and decoding are performed by physical systems, rather than by the execution of digital numerical algorithms. Chaotic optical systems have been demonstrated [11], and may potentially be used for ultra-high speed chaotic encryption.

*Ciphertext never repeats.* This is true even when the same plaintext is repeatedly encoded. This is a result of a basic property of chaotic systems: their state vector trajectory never repeats.

*Parasitic effects benefit security.* Encoding and decoding circuits must have matched components, but their values or detailed functional behavior need not be known. Consequently, matched electrical components fabricated side-by-side on a silicon wafer may exhibit "non-ideal" behavior due to parasitic device properties, but still perform encryption perfectly well.

*Plaintext is distributed between multiple ciphertext signals.* In order to decode a given plaintext stream, multiple ciphertext streams are required. It is possible to design a system where all components of the state vector of an *n*-dimensional encoding system are required to decode any one of the *n* plaintext streams.

*Continuous transmission is not required.* Ciphertext may be transmitted in intermittent spurts, for example. This is in contrast with the synchronization method, where each transmission of ciphertext must be long enough in duration for synchronization to occur.

*Does not exhibit cryptographic weaknesses of the synchronization technique that was analyzed in* [5]. The encoding chaotic system may be of high dimensionality. The plaintext need not be of small amplitude. A single attractor of the encoding system does not exist. It is possible to construct systems where the underlying equations approximating the system dynamics are extremely difficult, if not impossible, to determine.

*The physical environment comprises part of the key.* Circuits can be made that contain elements whose electrical function depends on environmental conditions, such as, for example, temperature (high temperature coefficient resistor), air pressure (micromachined piezoresistor), light intensity (photosensitive resistor), or acceleration (micromachined capacitor). If such components were appropriately incorporated in the circuits of Figs. 2 and 5, the plaintext would be correctly decoded only if the decoders simultaneously experienced the same temperature, light intensity, pressure, and acceleration as the encoder. In addition, the values of the other circuit elements (the other part of the key) must be correct.

*The term "computationally infeasible" acquires a new meaning.* If multiple aspects of the physical environment comprise part of the key, guessing the key may require producing many different environmental combinations. The process of creating multiple combinations of physical environments is typically slower than performing numerical computations, particularly for physical elements that exhibit hysteresis.

*There is great flexibility in implementation.* Physical systems that exhibit chaos include electrical, mechanical, electro-mechanical, electro-acoustic, or optical systems, for example. Mathematical implementations are also varied. Coupled differential equations exhibit chaos, as do coupled difference equations, for example. Though physical encryption systems are inherently analog, they can be used to encrypt digital data (just as a physical wire is used to transmit digital data).

## 5. Applications

Applications are myriad. A few include:

*Audio encryption.* The simple example circuit discussed earlier actually demonstrated audio encryption with minimal distortion. Audio frequency ciphertext such as that shown in Fig. 4 can be transmitted using the existing infrastructure for handling conventional audio signals.

*Environmentally sensitive locks.* The key to a conventional locking device can be encrypted, and the ciphertext recorded. Such a lock can be "opened" or "enabled" only if the correct ciphertext and correct environmental conditions are presented to the decoder.

*Tamper detector.* A decoder can be constructed such that parts of the decoding system actually comprise part of the physical system being monitored. If any part of the decoder is altered, it will not properly decode an encoded signal presented to it.

*High speed analog signal encryption.* Physical systems can be built whose short response times render them suitable for high speed encryption and decryption.

## 6. Summary

A new method to encrypt signals using chaotic systems has been demonstrated that offers security benefits over conventional chaotic encryption methods. The inherently analog nature of the method enables implementation methods for which conventional digitally-oriented cryptanalysis methods may not apply.

## Acknowledgments

The author is grateful to Chris Moorman for constructing the analog circuits, to Glenn LaVigne for experimental assistance, and to Bill Miller, Pete Gemmel, and Rush Robinett for stimulating discussions. This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy.

## References

1. E. Ott, C. Grebogi, and J. A. Yorke, Phys. Rev. Lett. **64**, 1196 (1990).
2. K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).
3. "Chaos in Communications", edited by L. M. Pecora, SPIE Vol. **2038** (1993).
4. Bianco et al., U.S. Patent #5,048,086; Cuomo et al., U.S. Patent #5,291,555; Gutowitz, U.S. Patent #5,365,589.
5. Th. Beth, D.e. Lazic, and A. Mathias, Advances in Cryptology - CRYPTO '94, in Lecture Notes in Computer Science Vol. **839**, p. 318, 1994.
6. L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).
7. L. M. Pecora and T. L. Carroll, Phys. Rev. **A 44**, 2374 (1991).
8. M. Ding and E. Ott, Phys. Rev. **E 49**, R945 (1994).
9. A. Maritan and J. R. Banavar, Phys. Rev. Lett. **72**, 1451 (1994).
10. S. L. Miller et al., Patent Pending.
11. Proceedings of the 1st Experimental Chaos Conference, Editors: S. Vohra, M. Spano, M. Shlesinger, L. Pecora, W. Ditto, World Scientific, New Jersey, 1992.