Ingeniería. Investigación y Tecnología
ISSN: 1405-7743
iit.revista@gmail.com
Universidad Nacional Autónoma de México
México

Núñez-Pérez, R.F.
Fuentes de corriente reducen a un canal la comunicación por encriptamiento caótico bidireccional
Ingeniería. Investigación y Tecnología, vol. XVIII, núm. 4, octubre-diciembre, 2017, pp. 353-368
Universidad Nacional Autónoma de México
Distrito Federal, México

*Ingeniería Investigación y Tecnología*
volumen XVIII (número 4), octubre-diciembre 2017 353-368
ISSN 1405-7743 FI-UNAM artículo arbitrado
Información del artículo: recibido: octubre de 2015, reevaluado: marzo de 2017, aceptado: abril de 2017


# Fuentes de corriente reducen a un canal la comunicación por encriptamiento caótico bidireccional

## *Current sources reduce to one channel the bidirectional chaotic encryption communication*

Núñez-Pérez R.F.

*Centro de Investigación Científica y de Educación Superior de Ensenada*
*Electrónica y Telecomunicaciones*
*Correo: rnunez@cicese.mx*

**Resumen**

Se muestra que un procedimiento basado en fuentes de corriente puede reducir el número de canales en un encriptador/desencriptador bidireccional, elaborado con un par de circuitos idénticos de Chua y sincronizados según Carroll y Pecora, este puede ser rentable y confiable. Se simula un circuito con el programa Workbench, se construye y evalúa su funcionamiento con algunas pruebas relevantes de ocultamiento y recuperación de mensajes de referencia e independientes. Dado que los resultados son aceptables y cumplieron con las principales características que debe respetar un circuito de este tipo, según la bibliografía especializada, el encriptador/desencriptador propuesto con un esfuerzo mínimo, se puede transformar para utilizarse con los circuitos de Lorenz, Chen y Rössler, entre otros, en un esquema novedoso de canales múltiples. Esto abonaría aun más la rentabilidad del mismo. También se vislumbra su aplicación en el campo de las comunicaciones digitales de baja frecuencia, específicamente en el envío bidireccional de mensajes binarios por medio de modulación paramétrica.

**Descriptores**: fuentes de corriente, circuito de Chua, encriptador/desencriptador caótico bidireccional.

***Abstract***

*Intends to show that a procedure based on current sources, can reduce the number of channels in an encryptor/decryptor bidirectional, performed with a pair of identical circuits of Chua and synchronized according to Carroll and Pecora, and therefore be cost-effective and reliable. Simulates the circuit with the Workbench program and is built and evaluated its operation with some evidence of concealment and retrieving messages from reference and independent. Given that their results were acceptable and met the main characteristics that must respect a circuit of this type, according to the specialized bibliography, the proposed encryptor/decryptor, with minimal effort, can be transformed for use with circuits of Lorenz, Chen, Rössler, among others, at a new scheme of multiple channels. This value even more the profitability of the same. Also, it sees its application in the field of low frequency digital communications, specifically in the bidirectional sent binary messages through parametric modulation.*

***Keywords****: current sources, Chua's circuit, bidirectional chaotic encryptor/decryptor.*

## Introducción

En el año 2001, se iniciaron actividades de simulación y experimentación con circuitos caóticos de Lorenz (Núñez, 2001) y de Chua (Chua, 1993; Matsumoto *et al*., 1985; Kennedy, 1992 y 1993; Núñez, 2006a y 2008) buscando realizar algunas aplicaciones en el campo de las comunicaciones encriptadas. Uno de los primeros desarrollos fue el comunicador bidireccional caótico que utilizaba los circuitos de Lorenz (Núñez, 2001 y 2006a; Shun *et al*., 2004) y tres líneas o canales para realizar su operación. Uno para sincronizar y los restantes para el envío de mensajes encriptados para cada dirección. El comunicador funcionó apropiadamente, pero no resultó rentable por el número de canales que utilizaba. En ese sentido, el presente trabajo propone una solución a esta necesidad de reducir el número de canales sin afectar las características principales de funcionamiento. Algunos autores como Cuomo *et al.* (1993a y b) han propuesto realizar la sincronización y el envío del mensaje encriptado (v.g., para un solo sentido) utilizando solo un canal, pero su procedimiento no es eficiente ni confiable como se ha demostrado, tanto teórica como experimentalmente por (Núñez, 2001, 2006a y 2006c; Corron y Hahs, 1997). Algunos otros como: Yongguang (2007) y Wagemakers *et al*. (2008) utilizan procedimientos de sincronización basados en cadenas de retardos y en procesos sincrónicos, respectivamente, los cuales son complejos. Otros autores como: Parlitz *et al*. (1992), Dedieu *et al*. (1993), Hasler and Schmming (2000), Posadas *et al*. (2004), Cruz *et al*. (2005), proponen la modulación paramétrica como un método seguro para el envío de mensajes binarios encriptados (v.g., para un solo sentido), pero no lo es tanto ya que, ante el *ruido* en el canal de comunicación, las señales encriptada y encriptadora son interferidas y es imposible recuperar fielmente la información binaria original, como se señala ampliamente en el estudio realizado por Núñez (2006b). Otros trabajos relevantes y actualizados sobre comunicaciones seguras bidireccionales son los de Guang *et al*. (2010) y Deng *et al*. (2009), los cuales se aplican particularmente a los láseres de semiconductor.

Considerando conceptos básicos de teoría de circuitos, se propone reducir el número de canales utilizando un circuito sencillo que trabaje en ***modo corriente***, para manejar, bidireccionalmente, los mensajes encriptados provenientes de una pareja de circuitos caóticos idénticos y sincronizados según el procedimiento de Carroll y Pecora (1991 y 1993). Así, es posible reducir el número de canales de dos a uno sin alterar la comunicación encriptada bidireccional; se piensa que por su sencillez, esto facilitará la implementación en el laboratorio y las aplicaciones del prototipo.

Para el caso de encriptado bidireccional por un solo canal en modo corriente, la bibliografía disponible es escasa, ya que solo se conoce el trabajo de Varrientos *et al*. (1995), quien presenta un esquema de mensajes encriptados caóticamente, de forma unidireccional que utiliza corriente; por lo que se cree que el trabajo original aquí propuesto podría interesar a los estudiosos del tema.

Existen varios circuitos caóticos (Moon, 1992; Buscarino *et al*., 2014) con los que se puede probar el procedimiento propuesto, de entre los cuales se seleccionó al de Chua (1993), (Matsumoto *et al*., 1985, Kennedy, 1992 y 1993, Chua *et al*., 1992) por su sencillez y no contener multiplicadores; también, se eligió para el convertidor de voltaje a corriente una fuente de corriente típica (Sepúlveda, 2010; Pease, 2008) aislada y con buena estabilidad. La simulación del circuito se realiza con el programa Workbench, se construye y prueba encriptando bidireccionalmente mensajes diferentes. También se averiguan los efectos que causa el ruido y la diafonía en la comunicación. En sí, el procedimiento basado en el circuito convertidor de voltaje a corriente puede utilizarse con cualquiera de los circuitos comunicadores caóticos que utilizan la sincronización de Carroll y Pecora (1991 y 1993).

Es conveniente mencionar que el análisis teórico del procedimiento de sincronización ya se realizó a detalle por Carroll y Pecora (1991 y 1993); Chua *et al*. (1992); Hasler (1994): Cruz *et al*. (2005); Posadas *et al*. (2004); Cuomo *et al*. (1993a y 1993b); Corron *et al*. (1997); Núñez (2001, 2006a y 2006c); Shun *et al*. (2004), entre otros.

En la segunda sección se presentan los fundamentos del circuito de Chua y su método de sincronización a través de la variable de estado o acoplamiento x1(Vx1); también, se citan algunos trabajos donde se estudia y califica este método y otros aspectos, tanto a nivel simulación como experimental. En la sección tres, se describe el circuito de encriptamiento/desencriptamiento bidireccional monocanal por fuentes de corriente propuesto para dos circuitos idénticos de Chua (Matsumoto *et al*., 1985; Kennedy, 1992 y 1993, Chua, 1993) y el funcionamiento de la fuente de corriente para el cometido de este estudio (Sepúlveda, 2010; Pease, 2008), respectivamente. En secciones 4 y 5, se presentan las simulaciones,construcción y pruebas experimentales realizadas al circuito mencionado con el programa Workbench dentro del laboratorio, asimismo el análisis/evaluación de los resultados de estas mismas, respectivamente (Álvarez y Shujun, 2006). Las pruebas de ocultamiento y recuperación bidireccional se realizan con señales apropiadas y se considera la acción del ruido eléctrico para validar mejor su comportamiento. Se califican los resultados con la me-

dición del factor de cresta y la distorsión armónica total de las señales en juego. Se describen los requisitos postulados por Alvarez y Shujun, 2006, que cumplen con el circuito de encriptador/desencriptador, posteriormente se plantea un esquema bidireccional múltiple que resulta ideal para los circuitos de Lorentz, Rössler y Chen, entre otros.

Finalmente, en la sección 6, se concluye con un circuito encriptador/desencriptador bidireccional que muestra la rentabilidad y confiabilidad que ofrece la utilización del canal de corriente con un par de circuitos idénticos de Chua sincronizados, según Carroll y Pecora (1991 y1993). Dicho circuito se utiliza con los circuitos de Lorenz, de Chen y de Rössler, entre otros, en un esquema novedoso de canales múltiples. Otra aplicación para este encriptador/desencriptador por corriente, es la del envío bidireccional de mensajes binarios por medio de modulación paramétrica (Núñez, 2006b; Parlitz *et al*., 1992; Dedieu *et al*., 1993; Hasler y Schming, 2000; Posadas *et al*., 2004; Cruz *et al*., 2005; Gámez y Cruz, 2008). Finalmente se presentan los agradecimientos y las referencias bibliográficas.

## Los circuitos de Chua y su sincronización

El circuito de Chua (Matsumoto *et al*., 1985; Kennedy, 1992 y 1993; Chua, 1993) también se conoce como de doble espiral, porque produce un atractor en el que su dinámica pasa de una espiral a otra. Es de tercer orden, autónomo, no lineal y disipativo, está compuesto por dos capacitores, un inductor, un resistor y un elemento no lineal. Este último es una conductancia lineal por segmentos, definida por la función $f(x_1)$ que se describe más adelante (ecuación 2). La dinámica del circuito se obtiene de las ecuaciones diferenciales normalizadas para el circuito de Chua A (transmisor)

$$\begin{aligned} dx_1/dt &= \alpha( x_2 - x_1 - f(x_1)) \\ dx_2/dt &= x_1 - x_2 + x_3 \\ dx_3/dt &= -\beta x_2 \end{aligned} \quad (1)$$

donde $x_2$, $x_1$, y $x_3$, son las variables de estado o señales que representan el voltaje a través de $C_2$, $C_1$, y la corriente en $L_1$, respectivamente. La falta de linealidad necesaria para el comportamiento caótico del circuito mencionado se obtiene de la función $f(x_1)$, llamada diodo de Chua (Matsumoto *et al*., 1985; Kennedy, 1992 y 1993; Chua, 1993). La cual se define

$$f(x_1) = bx_1 + 0.5(a - b)[| x_1 + 1| - | x_1 - 1|] \quad (2)$$

donde los valores típicos para los parámetros a y b son –1.27 y –0.68, respectivamente, y para $\alpha$ y $\beta$ son 10.0 y 14.9, respectivamente. En la figura 1, se muestra el diagrama eléctrico de los circuitos y diodos de Chua A y B etiquetados como transmisor y receptor, respectivamente; se acoplan y sincronizan vía canal 1. La literatura sobre estos circuitos y sus variaciones es muy abundante y se remonta desde mediados de los 80's (Matsumoto *et al*., 1985; Kennedy, 1992 y 1993; Chua, 1993; Chua *et al*., 1992) hasta la fecha.

## Sincronización

Las ecuaciones normalizadas de sincronización para el circuito B (') receptor, según Carroll y Pecora (1991 y 1993) y Chua *et al*. (1992 y 1993), son

$$\begin{aligned} dx_1'/dt &= \alpha'( x_2' - x_1' - f(x_1')) \\ dx_2'/dt &= x_1 - x_2' + x_3' \\ dx_3'/dt &= -\beta' x_2' \end{aligned} \quad (3)$$

donde su nomenclatura y valores son iguales a los del circuito A transmisor. Como se observa en (1) y (3), se

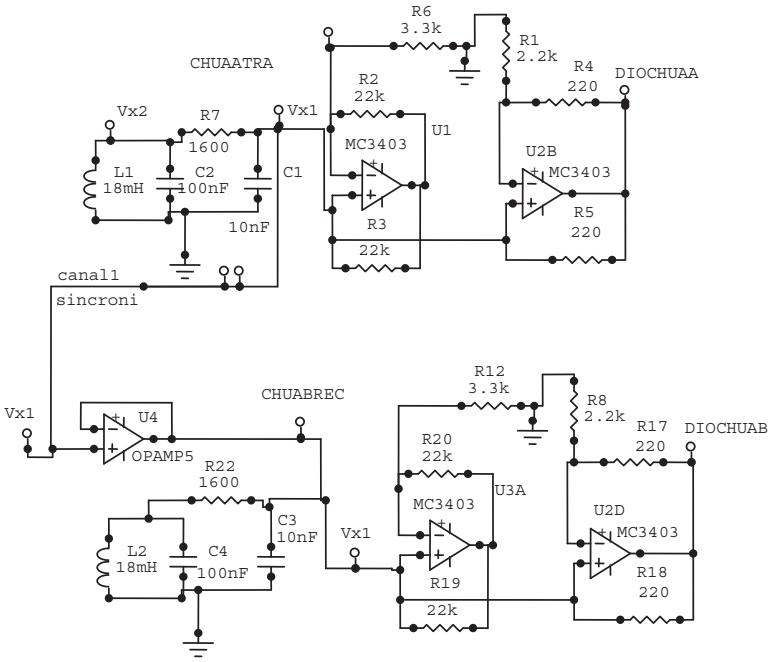


Figura 1. Diagrama eléctrico de los circuitos de Chua A (transmisor) y B (receptor) mostrando el canal 1 de sincronización vía la señal de acoplamiento Vx1 (Carroll y Pecora, 1991 y 1993)

sabe de Carroll y Pecora (1991 y 1993) y de otros (Matsumoto *et al*., 1985; Kennedy, 1992 y 1993, Chua, 1993; Chua *et al*., 1992; Hasler, 1994; Varrientos *et al*., 1995), solamente se puede sincronizar directamente por medio de las variables de estado $x_1$ y $x_2$. Para este caso, se utiliza $x_1$ para acoplar y sincronizar ambos circuitos idénticos.
La función del diodo de Chua para este caso es

$$f(x_1') = bx_1' + 0.5(a - b)[|x_1' + 1| - |x_1' - 1|], \quad (4)$$

donde los valores típicos para los parámetros a y b son –1.27 y –0.68, y para α′ y β′ son 10.0 y 14.9, respectivamente.

Con la finalidad de facilitar la explicación, las variables de estado se representan por señales de voltaje en los circuitos sincronizados del diagrama eléctrico de la figura 1. Por ejemplo, se tiene para el circuito A transmisor (CHUAATRA): x1= Vx1, x2= Vx2, y para el circuito B (′) receptor (CHUABREC): x1= Vx1 y x2′= V′x2.

El análisis teórico-experimental de los diferentes métodos de sincronización para este tipo de circuitos lo han realizado: Carroll y Pecora (1991 y 1993); Chua *et al*. (1992); Hasler (1994); Cruz *et al*. (2005); Cuomo *et al*. (1993a y b); Corron *et al*. (1997); Núñez (2001, 2006a y 2006c); Shun *et al.* (2004); Yongguang (2007); Wagemakers *et al*. (2008); López y Cruz (2005); Milanovi'c y Zaghloul (1996) entre otros, y dentro de los procedimientos teórico-experimentales más utilizados para calificar el grado y la robustez en las sincronizaciones se pueden citar las comparaciones de formas de onda (Núñez, 2001, 2004 y 2008), de firmas espectrales (Núñez, 2001, 2006c y 2009), de planos de fase o atractores (Núñez, 2001, 2006c y 2009), de riquezas espectrales (Núñez, 2009), de cuantificadores del caos del circuito de Chua (Núñez, 2008), de encriptado/desencriptado de información binaria (Núñez, 2008), de funciones de análisis de coherencia (Núñez, 2004), entre otros.

## Circuito encriptador/desencriptador caótico bidireccional monocanal por fuentes de corriente

Uno de los primeros desarrollos realizados en este campo, fue el comunicador bidireccional caótico que utilizaba circuitos de Lorenz (Núñez, 2001 y 2006a, Shun *et al*., 2004) y tres líneas, o canales, para realizar su operación. Uno para sincronizar y los otros dos para el envío de los mensajes encriptados en ambos sentidos y en forma independiente. El comunicador funcionó apropiadamente en el laboratorio, pero al tratar de aplicarlo fuera del mismo ya no resultó tan rentable por el número de canales que utilizaba, en vista de ello, el presente trabajo propone reducir el número de canales en aras de no afectar el rendimiento del comunicador.

Considerando conceptos básicos de teoría de circuitos, se propone reducir el número de canales utilizando un circuito sencillo que trabaja en modo corriente (Sepúlveda, 2010; Pease, 2008) para manejar bidireccionalmente, i.e., por un solo canal los mensajes encriptados provenientes de una pareja de circuitos caóticos idénticos, como se muestra en la figura 2.

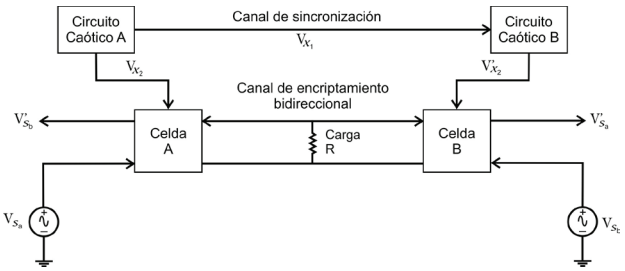


Figura 2. Diagrama a cuadros del encriptador/desencriptador caótico bidireccional monocanal por fuentes de corriente propuesto

El procedimiento de ocultamiento y recuperación de los mensajes enviados en forma bidireccional se describe apoyándose en el diagrama a cuadros y en el funcional mostrado en las figuras 2 y 3, respectivamente.

Para facilitar la descripción, se inicia tratando el caso de la recuperación del mensaje V′sb, que envía el circuito caótico de la celda B al de la A y que se oculta por la señal encriptadora Vb cuando se suman las señales Vsb (original) y caótica V′x2 (i.e., Vb= Vsb + V′x2). Por otro lado, el circuito caótico de la celda A hace lo propio, generando una señal Va que encripta el mensaje original Vsa cuando este se suma a la señal caótica Vx2 (i.e., Va= Vsa + Vx2). Aquí se encuentra la clave de la propuesta, estas señales encriptadoras Va y Vb se convierten a corrientes por medio de los convertidores de V/I (i.e., tensión/corriente, T/C) en cada uno de los circuitos mencionados. Por ello, para el circuito de la celda A, la Ia corresponde a la suma de las corrientes Isa e Ix2 (i.e., Ia= Isa + Ix2). Dicha corriente, se suma a la Ib proveniente del circuito de celda B, que es la suma de las corrientes Isb e I′x2 (i.e., Ib= Isb + I′x2), y se produce la señal auxiliar Vc (i.e., Vc= R (Ia + Ib)= Va + Vb), que es un voltaje que aparece en la resistencia común de carga R, y el cual alimenta al canal llamado de encriptamiento/desencriptamiento bidireccional.

Ahora bien, para recuperar el mensaje V′sb que viene oculto por V′x2, a la señal auxiliar Vc, se le resta la señal encriptadora Va en el circuito caótico de la celda A (i.e., Vb= Vc - Va), y así se obtiene la señal encriptadora Vb. Como esta es la suma de V′x2 y Vsb, entonces al

restarle Vx2 del mismo circuito (i.e., V'sb= Vsb + V'x2 – Vx2) se recupera V'sb; dado que los circuitos caóticos de las celdas A y B son idénticos y sincronizados por la señal de acoplamiento Vx1; a través del canal correspondiente se tiene que Vx2 y V'x2 son aproximadamente iguales. De esta forma, se recupera el mensaje oculto que proviene del circuito caótico de la celda B.

Para recuperar el mensaje oculto V'sa que envía el circuito caótico de la celda A a la B, se realiza un procedimiento semejante, pero en el circuito caótico de la celda B. Ambas recuperaciones de las señales de mensajes originales Vsa y Vsb se realizan en tiempo real. En la figura 9 se presenta el diagrama eléctrico del circuito diseñado que corresponde solo a la sección del transmisor de Chua A, la otra sección no se presenta por cuestiones de espacio.

Para el caso experimental de laboratorio, solo será exitoso si la sincronización (i.e., realizada por el canal correspondiente) no se pierde, los convertidores de V/I o T/C (v.g., constituidos por los operadores analógicos U1D y U2A de la figura 9) se mantienen lineales y los canales captan el menor ruido posible. Aunque por tratarse de corrientes en el canal de encriptamiento, estas presentan una menor susceptibilidad por ser interferidas electromagnéticamente en comparación con las de voltaje del canal de sincronización.

### La fuente de corriente y su utilización

La fuente de corriente o convertidor de voltaje a corriente empleado, se controla por voltaje (Sepúlveda, 2010; Pease, 2008) y su ecuación característica se rige por la ley de Ohm, como se muestra en la figura 9 y en las siguientes expresiones.

Las ecuaciones del circuito son

del nodo v(+):

$$(V - Va)/R14 + (V - Vc)/R15 = 0 \quad (5)$$

despejando Vc se obtiene

$$2V - Va = Vc$$

del nodo v(–)

$$V/R13 + (V - Vs)/R16 = 0$$

despejando Vs se obtiene

$$2V = Vs$$

Ahora, tomando la corriente que pasa por la resistencia R17 se obtiene

$$(Vs - Vc)/R17 = Ia$$

sustituyendo Vs y Vc en la ecuación anterior se tiene

$$Va/R17 = Ia$$

con lo que se constata que existe una relación lineal entre la corriente de salida Ia y el voltaje de entrada Va. Las principales características de la fuente de corriente son: su buena estabilidad y que sus regresos pueden ser independientes para el voltaje de entrada y la corriente de salida.

## Pruebas al circuito propuesto utilizando diversos mensajes bidireccionales

### Simulación del circuito con el programa Workbench (Wb)

El circuito propuesto de encriptamiento/desencriptamieto bidireccional por fuentes de corriente se simula con el programa Wb. Para realizar las pruebas se definieron los circuitos caóticos sincronizados como: Chua A (celda A-transmisor) y Chua B (celda B-receptor), estos consisten en:

a) Encriptar/desencriptar señales diferentes en ambos sentidos.
b) Desplegar el error en la sincronía o asincronía por dirección y
c) Encriptar/desencriptar una misma señal, o de autoprueba (v.g., este caso no se presenta).

La prueba de encriptar/desencriptar señales diferentes en ambos sentidos es representativa y manifiesta, al final de cuentas, el potencial del procedimiento propues-

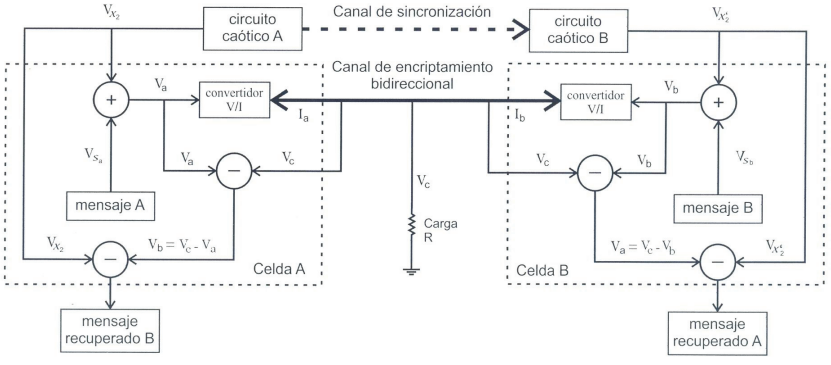


Figura 3. Diagrama funcional del encriptador/desencritador caótico bidireccional propuesto. Para la descripción particular, se indican las señales de sincronización del mensaje original Vsb (celda B), de encriptamiento V'x2 (celda B) y del mensaje recuperado por el Chua A (celda A) V'sb

to. Se proponen como señales de mensaje de prueba una cuadrada Vsa y una senoidal Vsb con 0.1 y 0.15 Vp de magnitud, respectivamente. Ambas a una frecuencia de 1KHz.

En las partes superior e inferior de la figura 4, se despliegan las formas de onda de las señales mencionadas. En la figura 5 se presentan las correspondientes señales recuperadas V'sa y V'sb, que al compararlas con las originales de la figura anterior resultan ser bastante parecidas. Por otro lado, en las figuras 6 y 7 se presentan la señal recuperada V'sa y su encriptadora Va (v.g., Va= Vsa + Vx2), para el envío del circuito caótico de la celda A a la B, y la señal caótica Vx2 (i.e., en la parte superior) y la encriptadora Va, respectivamente. En la figura 8, se presenta el error en la sincronización por dirección de envío de mensaje para Vsa y Vsb en la parte superior e inferior, respectivamente. Dicha asincronía, es básicamente la diferencia de Vx2 y V'x2 por cada dirección, puesto que las magnitudes de las señales del mensaje original (v.g., la Vsa y la Vsb) se redujeron a cero voltios para esta prueba.

## Pruebas de funcionamiento al circuito en el laboratorio

Se realizan pruebas al circuito realizado y se valida su funcionamiento. En la figura 9 se presenta la parte del circuito que corresponde a la celda A, también llamado transmisor. Buscando la consistencia, se propusieron señales de prueba muy semejantes a las utilizadas en la simulación con el programa Wb, las cuales se presentaron anteriormente. Esto se puede constatar por medio del grupo de fotografías presentadas en las figuras 10-13; dichas fotografías muestran las series de mediciones practicadas al circuito. Se refuerza lo anterior con las mediciones y cálculos que se exhiben en la carátula interfaz hombre-máquina del instrumento virtual LabVIEW7-PMD1208LS (Núñez, 2008) de la figura 14.

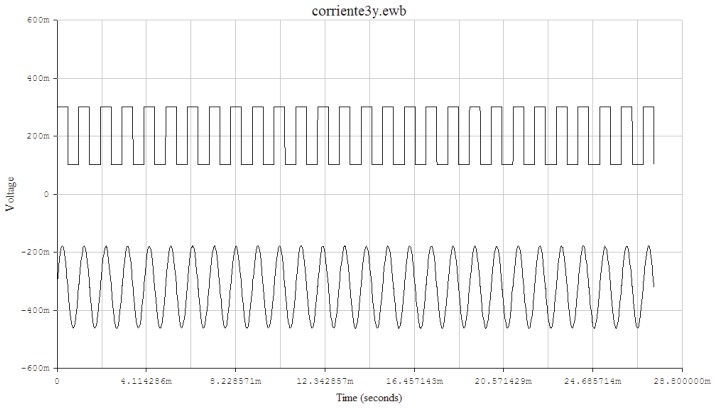


Figura 4. Señales originales de mensajes de prueba: cuadrada Vsa (superior) y senoidal Vsb con magnitudes de 0.1 y 0.15 Vp, respectivamente. Ambas a 1KHz

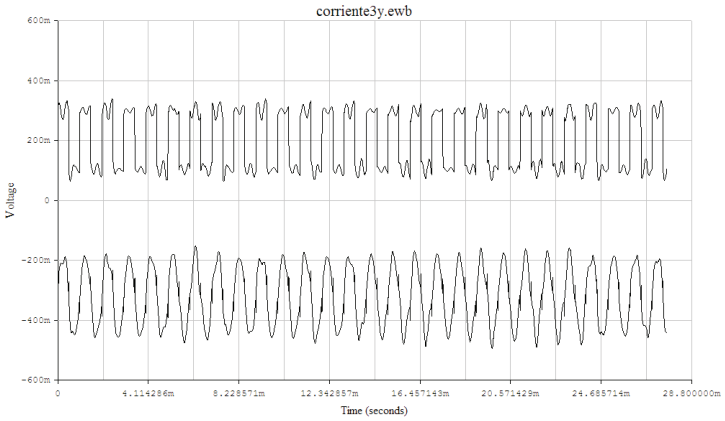


Figura 5. Señales de mensajes recuperados V'sa (superior) y V'sb, se observa la distorsión en la amplitud impuesta por la asincronía

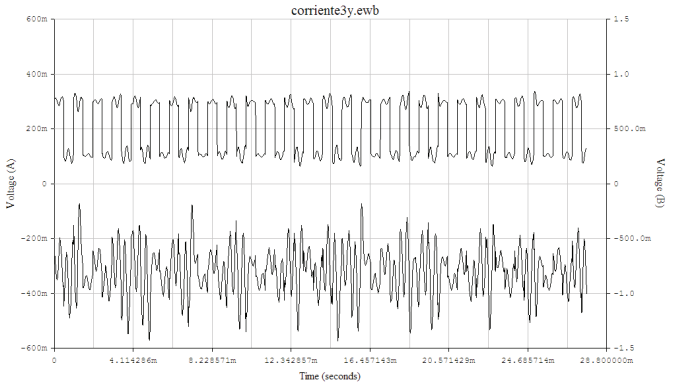


Figura 6. Señales de mensaje recuperado V'sa (superior) y encriptadora Va (Va= Vsa + Vx2)

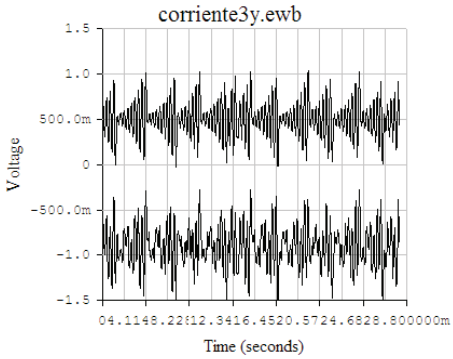


Figura 7. Señales caótica Vx2 (superior) para encriptar y encriptadora Va

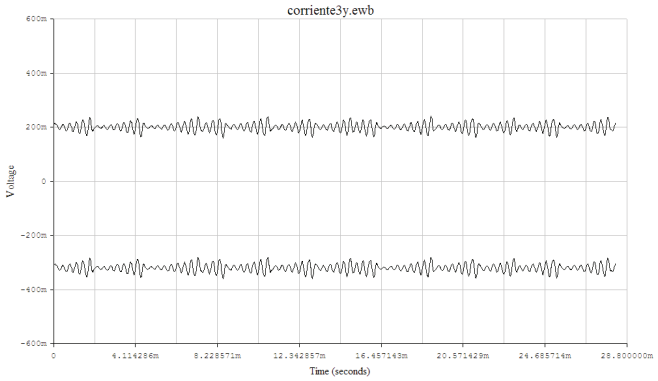


Figura 8. Señales de asincronía correspondientes a la dirección de los mensajes Vsa (superior) y Vsb; la magnitud de estas señales es cero voltios

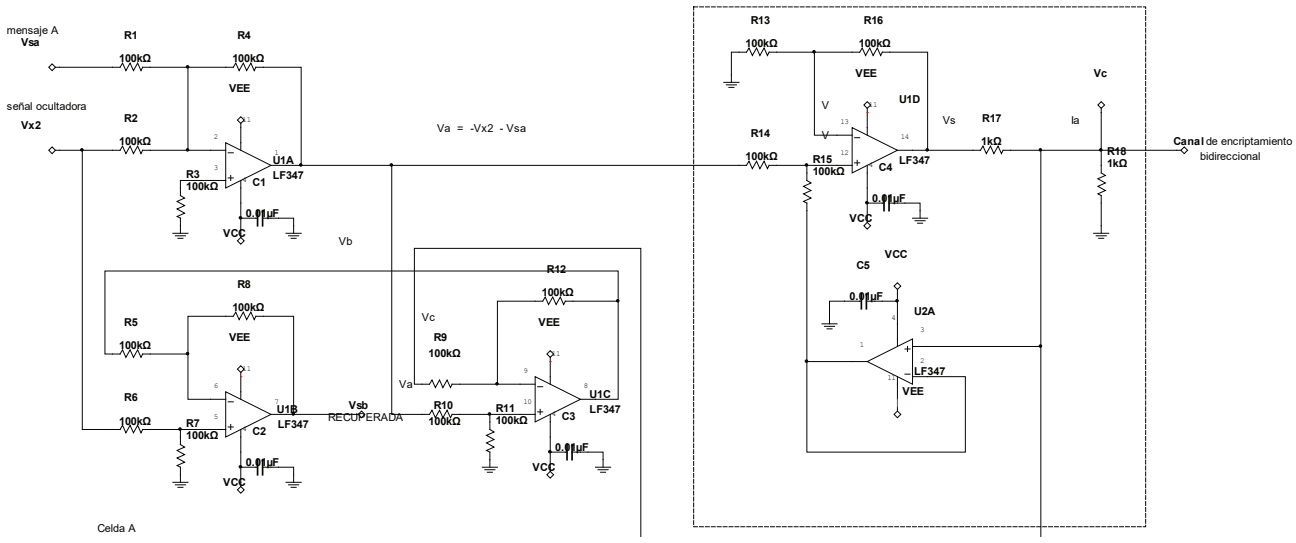


Figura 9. Diagrama eléctrico del circuito encriptador/desencritador caótico correspondiente a la celda A (transmisor)

Por facilidad en el análisis, síntesis e interpretación de los resultados, se seleccionan las señales de mensaje senoidal y cuadrada con magnitudes y frecuencias de 100 mVp y 50mVp y de 1 KHz, de 0.2 KHz y de 0.5 KHz, respectivamente. Para el caso de la simulación presentada en la sección de simulación del circuito con el programa Work bench (Wb), se consideran la magnitud y la frecuencia de 100mV y de 1 KHz, respectivamente, para ambas señales de mensaje. Los sentidos en los que se envían los dos tipos de señales son: la cuadrada va de la celda A a la B y la senoidal va de la celda B a la A. Las señales ocultadoras son las mismas caóticas Vx2 y V'x2, mencionadas en la simulación, cuyas magnitudes y frecuencias se encuentran en la vecindad de 1 Vp y 6.25 KHz, respectivamente. En la figura 10 se muestra en la parte superior de la pantalla del osciloscopio, las señales del mensaje enviado Vsb y su correspondiente recuperado V'sb, asimismo en la parte inferior de la misma, y en el mismo orden, se presenta el mensaje enviado de Vsa y su correspondiente recuperado V'sa; todo en funcionamiento bidireccional, en tiempo real y a frecuencias de 200 Hz. Como se contempla, algunos de estos resultados son semejantes a los obtenidos en la simulación y presentados en las figuras 4 y 5.

En la figura 11 se muestra, en la parte superior de la pantalla del osciloscopio, las señales del mensaje enviado Vsb y su correspondiente recuperado V'sb. En la parte inferior de la misma, y en el mismo orden, se presenta la señal ocultadora Va del mensaje Vsa (Va= Vsa + Vx2) y su correspondiente recuperado V'sa; funcionando bidireccionalmente y en tiempo real. Para este caso se elige la frecuencia de 200 Hz para las señales en juego. Como se observa, estos resultados son semejantes a los obtenidos en la simulación, presentados en las figuras 4, 5 y 6.

En la figura 12 se muestra en la parte superior de la pantalla del osciloscopio, las señales del mensaje enviado Vsb, y su correspondiente recuperado V'sb, asimismo en la parte inferior, y en el mismo orden, se presenta la señal ocultadora Va del mensaje Vsa (Va= Vsa + Vx2) y la señal caótica Vx2; en funcionamiento bidireccional, en tiempo real y a frecuencias de 1 KHz. Como se puede apreciar, estos resultados son semejantes a los obtenidos en la simulación presentados en las figuras 4, 5 y 7.

En la figura 13 se muestran en la parte superior de la pantalla del osciloscopio, las señales del mensaje enviado Vsb, y su correspondiente recuperado V'sb; en la parte inferior de la misma y en la parte central, se presenta el error en la recuperación er= Vsb – V'sb. Las magnitudes de las señales mencionadas se escogen para este ejercicio de 50 mVp para las señales del men-

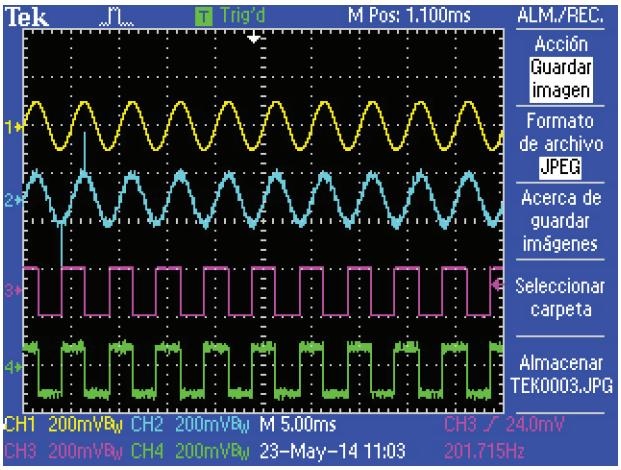


Figura 10. Se muestran en orden descendente las señales del mensaje enviado Vsb, del recuperado V'sb, del mensaje enviado Vsa y del recuperado V'sa; todo en funcionamiento bidireccional y en tiempo real Fs= 200Hz

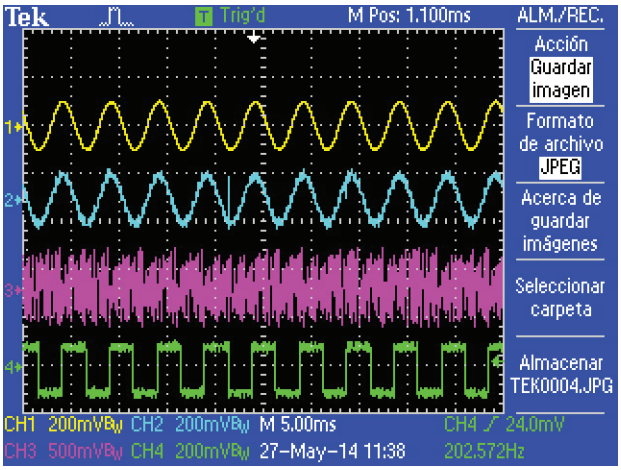


Figura 11. Se muestran en orden descendente las señales del mensaje enviado Vsb, del mensaje recuperado,V'sb, la señal caótica encriptadora del mensaje Vsa y el mensaje recuperado V'sa, en forma bidireccional y en tiempo real Fs= 200Hz

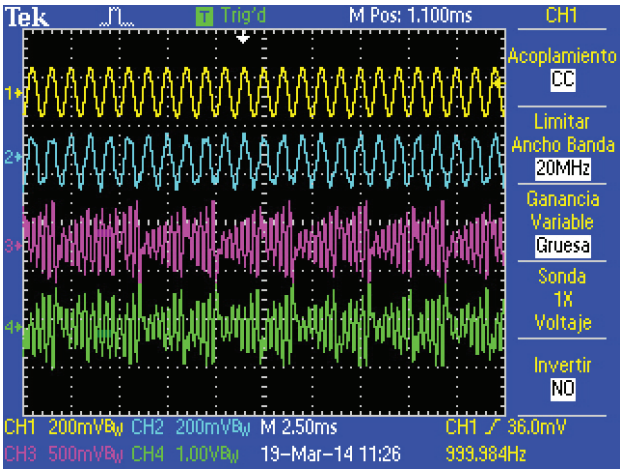


Figura 12. Se muestra en la pantalla del osciloscopio, parte superior, las señales del mensaje enviado Vsb y su correspondiente recuperado V'sb, y en la parte inferior de la misma, se presenta la señal ocultadora Va del mensaje Vsa (Va= Vsa + Vx2) y la señal caótica Vx2, en forma bidireccional y en tiempo real Fs= 1KHz

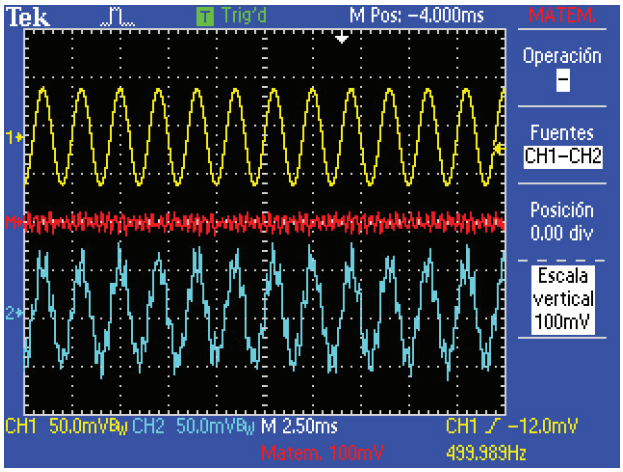


Figura 13. En las partes superior e inferior de la pantalla del osciloscopio se muestran las señales del mensaje enviado Vsb y su correspondiente recuperado V'sb, respectivamente. En el centro se presenta el error en la recuperación er=Vsb-V'sb. Canales 1 y 2: 50mV/cuadro y canal de error: 100mV/cuadro Fs= 500 Hz

saje y, por consecuencia, la magnitud del error que se mide es de aproximadamente 10 mVp. Para este caso, se utilizan frecuencias de 500 Hz. De nuevo los resultados son equivalentes a los de la simulación, que se presentaron en las figuras 4, 5 y 8.

Se utiliza la carátula interfaz hombre-máquina, presentada en la figura 14 por el instrumento virtual LabVIEW7-PMD1208LS (Núñez, 2008), para desplegar las señales del mensaje original y del recuperado Vsb y V'sb, respectivamente, en el cuadro izquierdo, así como sus espectros, en el derecho. También se reporta la calidad relativa de la recuperación del mensaje original con base en el cálculo del *factor de cresta* (FC) y de la *distorsión armónica total* (DAT, en inglés: THD) para cada una de las señales medidas en tiempo real (Núñez, 2014). Los índices seleccionados ayudan a calificar la calidad de las señales recuperadas al compararse con los de las originales. Para la prueba, se escoge una frecuencia de 200 Hz para las señales en juego. En la tabla 1, se presentan los valores de estos calificadores del proceso de recuperación para la señal del mensaje original y el de la recuperada.

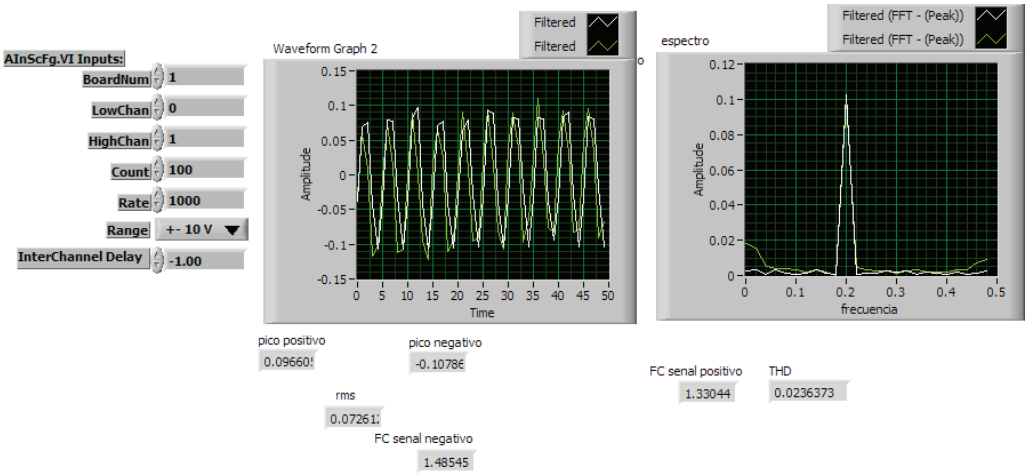


Figura 14. El instrumento virtual LabVIEW7-PMD1208LS muestra los mensajes original Vsb y el recuperado V'sb de forma traslapada en la ventana izquierda, así como sus espectros correspondientes. En la siguiente, la calidad relativa en la recuperación se obtiene al comparar los índices: FC (señal positiva) y DAT (THD) de las señales en juego Fs= 200 Hz

Tabla 1. Calidad relativa de la recuperación del mensaje V'sb, basada en el FC y la DAT de las señales

| Señal de mensaje(Vsb) [mVp] | Factor de cresta: FC[adimensional] | Distorsión armónica total:DAT[adimensional] |
|---|---|---|
| Original (Vsb) | 1.37 | 0.021 |
| Recuperada (V'sb) | 1.33 | 0.024 |
| Error (er= Vsb–V'sb) | 0.04 ( 3%) | –0.003 (–14%) |

Se propone otra prueba, pero esta vez en alta frecuencia para averiguar el comportamiento del circuito encriptador cuando el mensaje es la misma señal cuadrada original Vsa, pero ahora a 300 KHz. En la figura 15, se muestra la señal caótica Vx2 (superior) y la señal encriptadora Va que es la suma de Vx2 y la señal mensaje de prueba Vsa (i.e., la cuadrada a 300 KHz) (c.f., con las figuras 7 y 11). Como se observa, Vsa no se encripta solo se mantiene sobre el perfil de Vx2. En la figura 16 se presentan los resultados del rendimiento en la recuperación del mensaje original Vsa, el cual como puede constatarse (V'sa) no es muy bueno (c.f., con las figuras 4, 5, 6, 10 y 11).

En la figura 22 se presenta la maqueta de prueba que se utiliza para evaluar experimentalmente al circuito propuesto.

Finalmente, para dar más certidumbre al procedimiento de encriptamiento propuesto y considerando las mismas señales de las figuras 15 y 16, se despliega la firma espectral de la señal caótica encriptadora Vx2 con la idea de exhibir la región de utilidad para la labor de encriptamiento (Núñez, 2006a y b). Para esta prueba, se utiliza la misma señal de prueba Vsa cuadrada de 1 KHz, mencionada en las figuras anteriores, con una magnitud mayor a la normal por encriptar, con la idea de mostrar lo que sucede con la fundamental y sus armónicas al enmascararse por la firma espectral de Vx2 (i.e., se realiza algo parecido a un barrido espectral). En la figura 17 se presentan en orden descendente, las señales Vx2, Vsa, Va y V'sa correspondientes a la caótica de 700 mVp, a la señal cuadrada de prueba de 100 mV, a la encriptadora (i.e., Va= Vsa + Vx2) y a la recuperada (i.e., V'sa= Va – V'x2= Vsa + Vx2 – V'x2) en el receptor B (c.f., con el diagrama a cuadros funcional de la figura 3), respectivamente. En las figuras 18-21 se despliegan, en el mismo orden que el de la figura 17, los espectros de las señales mencionadas.

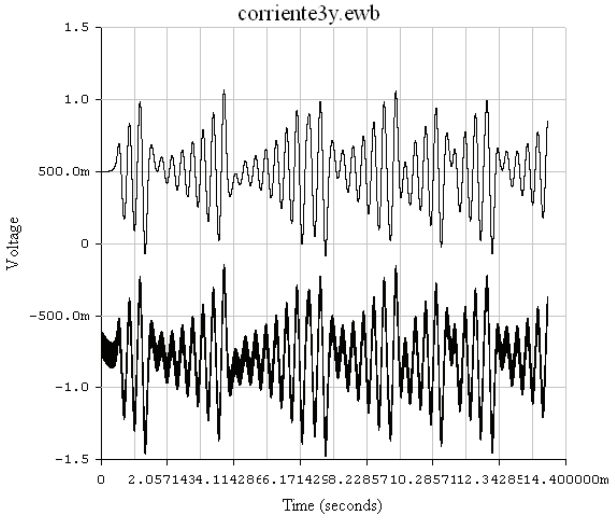


Figura 15. Muestra la señal caótica Vx2 (superior) y la señal encriptadora Va, que es la suma de Vx2 y la señal mensaje original Vsa (i.e., la cuadrada y bajo prueba a 300 KHz) (c.f., con las figuras 7 y 11). Como se observa, Vsa no se encripta solo se mantiene sobre el perfil de Vx2

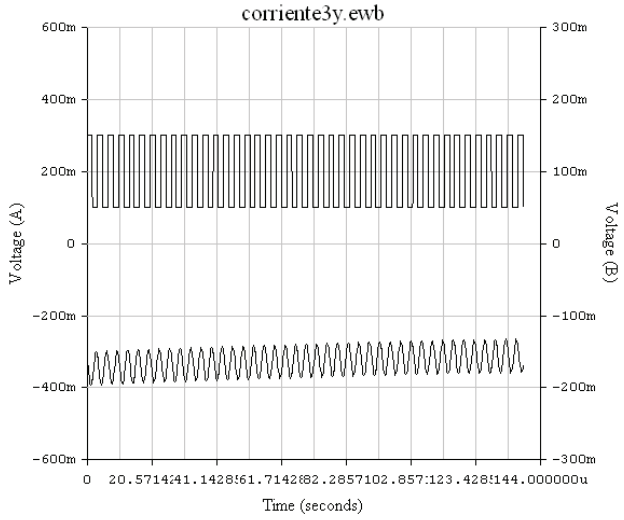


Figura 16. Señal original del mensaje enviado (i.e., Vsa cuadrada a 300 KHz) y recuperado V'sa (inferior). Se observa que, pese a que Vsa no se encriptó, el circuito filtra y distorsiona (c.f., con las figuras 4, 5, 6, 10 y 11)

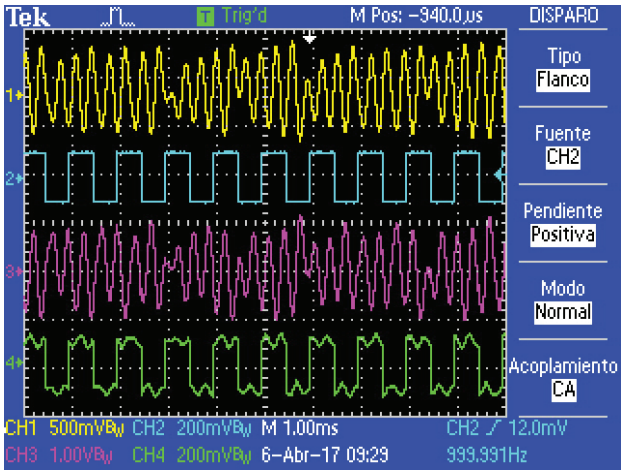


Figura 17. En orden descendente, las señales Vx2, Vsa, Va y V'sa corresponden a la caótica de 700 mVp, a la señal cuadrada de prueba de 1 KHz y 100 mV, a la encriptadora (i.e., Va= Vsa + Vx2) y a la recuperada (i.e., V'sa= Va – V'x2= Vsa + Vx2 – V'x2) en el receptor B, respectivamente

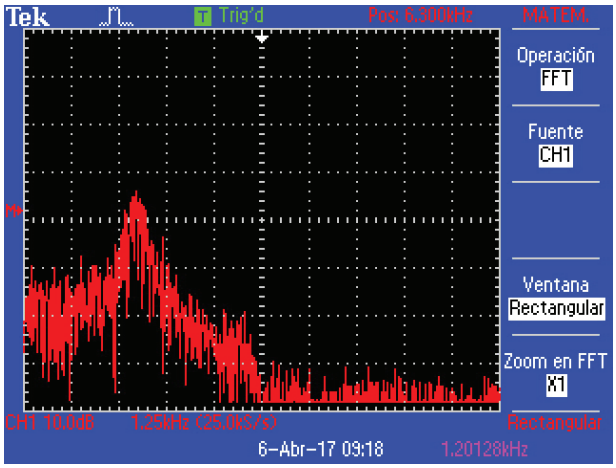


Figura 18. Firma espectral de la señal caótica Vx2, mostrando su mascarilla útil para encriptar señales de 0.10 a 6.25 KHz (i.e., un barrido de 0.08*1.25 KHz/cuadro a 1.25 KHz/cuadro*5 cuadros)

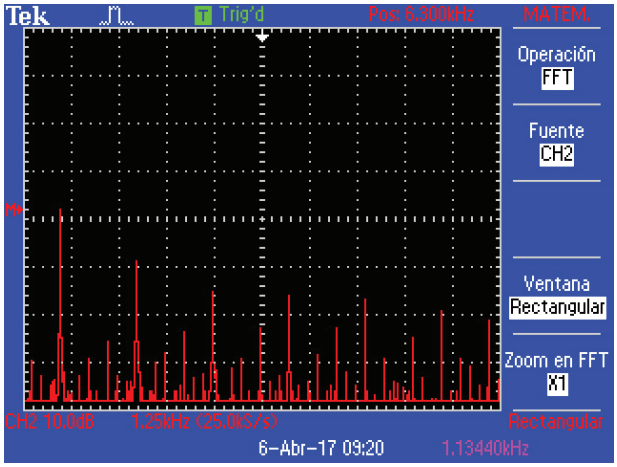


Figura 19. Espectro de la señal cuadrada de prueba Vsa de 1 KHz (i.e., la fundamental en 0.8*1.25 KHz/cuadro) y 100 mV

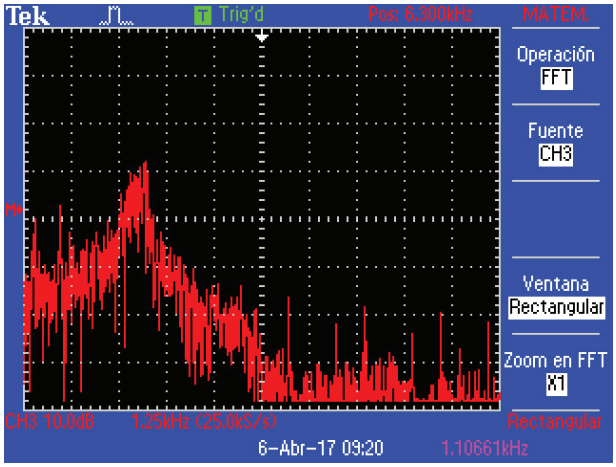


Figura 20. Firma espectral de la señal encriptadora Va (i.e., Va= Vsa + Vx2), solo las dos primeras armónicas (i.e., la de 3 y 5 KHz) de Vsa se ocultan completamente, mientras la fundamental lo hace parcialmente, el resto permanece igual (i.e., las de 7, 9 y 11 KHz)

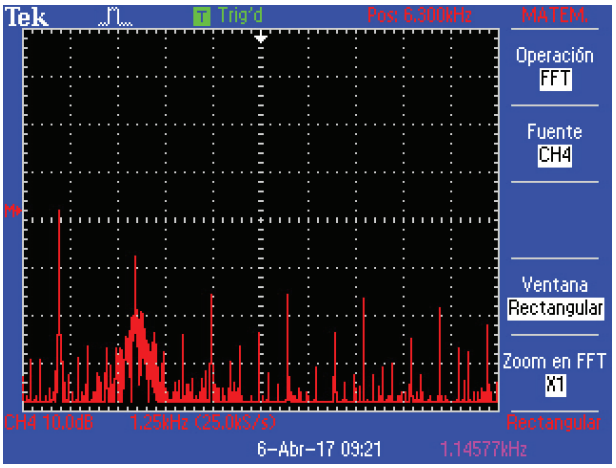


Figura 21. Espectro de la señal cuadrada de prueba V'sa recuperada en el receptor B. Pese a que la primera armónica (i.e., la de 3 KHz, 3*0.8*1.25 KHz/cuadro) presenta algo de ruido, la recuperación en general, es aceptable (c.f., con la figura 19)

## Análisis y evaluación del encriptamiento/desencriptamiento de mensajes bidireccionales

### Discusión de los resultados de la simulación con el Wb

El análisis del estudio comparativo entre las señales recuperadas y las originales arroja una calidad aceptable, la distorsión en la amplitud se debe principalmente a la asincronía. Es claro entender por que V'sa se distorsiona más que la señal V'sb, ya que se trata de una forma de onda cuadrada (Álvarez y Shujun, 2006; López y Cruz, 2005; Milanovi'c y Zaghloul, 1996). Como se observa en la parte baja de la figura 6, la señal encriptadora Va cumple su misión al no permitir que se observe rastro del mensaje original Vsa encriptado. Por lo que se puede decir que el encriptamiento proporcionado por la señal Vx2 es aceptable; pese a que su riqueza espectral (Núñez, 2009) es mucho menor que la de la señal Vx1 (Kennedy, 1992 y 1993; Chua, 1993). Respecto al despliegue de la asincronía por canal bidireccional mostrado en la figura 8, se observa que esta es pequeña porque presenta una magnitud de alrededor de 20 mVp y, por lo tanto, es 35 veces menor que la de la señal caótica encriptadora Va, es decir, cerca de 700 mVp (c.f., con la figura 7).

### Discusión de los resultados experimentales en el laboratorio

Al igual que en la sección de la discusión de los resultados de la simulación con el Wb, los resultados experimentales son aceptables (figura 10), las señales Vsa, Vsb y sus correspondientes recuperadas, son medidas con distorsiones menores como se observa en la figura 14. Estas se encuentran en la vecindad de los 20 mVp (c.f., la señal central de la figura mencionada, con escala de 100mV/cuadro) que si se compara con las magnitudes de las señales encriptadoras Va y Vb, del orden de 700mVp (c.f., figura 12) resulta ser de 35 veces menor. Lo digno de resaltar es la semejanza que se registra entre los resultados de la simulación y las mediciones experimentales (c.f., figuras 5, 8 y 13); el error en las recuperaciones es semejante al de la asincronía entre los circuitos = Vc2 - V'c2.

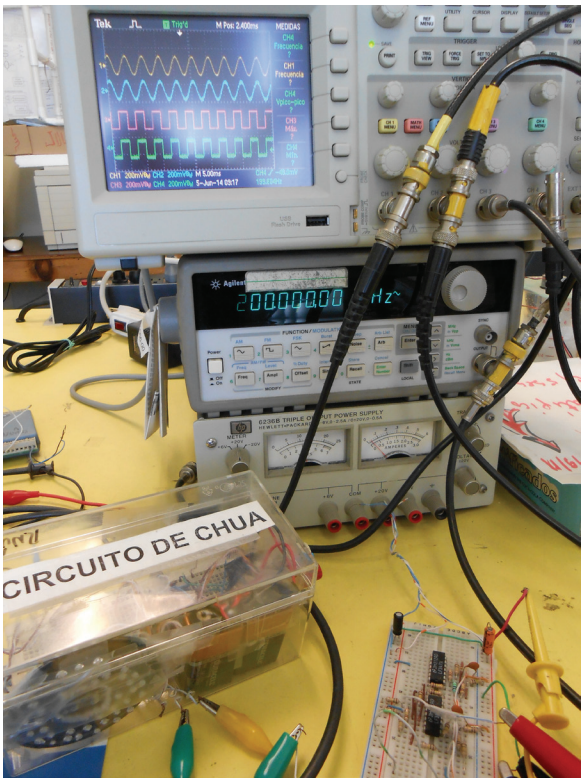


Figura 22. Maqueta de prueba con circuito propuesto en evaluación experimental

Por otro lado, la calidad relativa de la recuperación del mensaje original se obtiene cuantitativamente al comparar los índices de los factores de cresta y de la distorsión armónica total de las señales originales y recuperadas. En la tabla 1 se presentan resultados de la prueba para cuando las señales, enviada Vsb y recuperada V'sb, son senoidales de 100mVp y de 200 Hz en ambos sentidos de operación y en tiempo real, como lo indican las mediciones del instrumento virtual LabVIEW7-PML1802. Los errores en diferencias y porcentuales son: FC= 0.04 (3%) y DAT= –0.003 (–14%), los

cuales corroboran los errores en la sincronización, mencionados en la sección de discusión de los resultados de la simulación con el Wb.

La prueba realizada para averiguar el comportamiento del circuito encriptador en alta frecuencia, cuando el mensaje es la misma señal cuadrada original Vsa, pero a 300 KHz, se presenta en la figura 15. En esta, se observa que Vsa no se encripta sino se mantiene cabalgando sobre el perfil de Vx2. Los resultados en la recuperación del mensaje original Vsa no resultan ser buenos (c.f., figuras 4, 5, 6, 10 y 11), puesto que el mensaje V'sa aparece filtrado y distorsionado como lo indica la figura 16.

Respecto a la prueba realizada para dar certidumbre al procedimiento propuesto, en la figura 18 se observa que la firma espectral de Vx2 se constituye por un espectro quebradizo y carente de zonas planas. Para el caso particular, se propone un ancho útil máximo o mascarilla de encriptamiento de 0.10 a 6.25 KHz (i.e., de 0.08*1.25 KHz/cuadro a 1.25 KHz/cuadro*5 cuadros) que considera solo armónicas mayores a 10 dB (c.f., figuras 19 y 21). Al analizar la afirma espectral de la señal encriptadora, i.e., Va= Vsa + Vx2, presentada en la figura 20, se puede constatar que solo las dos primeras armónicas ( i.e., 3 y 5 KHz) de Vsa (c.f., figura 19) se ocultan completamente, mientras que la fundamental lo es parcialmente (i.e., 1 KHz) y el resto de las armónicas permancen iguales. Esto se esperaba por la magnitud elegida para la señal de prueba Vsa (i.e., 100 mV y que es más del doble de lo que normalmente se utiliza para el encriptamiento) (c.f., figura 17), respecto a la de la señal caótica Vx2. Como se observa en la figura 21, la recuperación de la señal Vsa, i.e., la señal V'sa (c.f., figura 19), es aceptable, puesto que la fundamental y sus armónicas así lo indican; solo la primera armónica presenta una pequeña interfencia (i.e., 3 KHz), que también se puede observar en su representación correspondiente de la figura 17.

## Comentarios, mejoras y pronósticos

A manera de completar y validar el análisis del estudio comparativo realizado, se puede mencionar que el circuito propuesto cumple con algunos requerimientos básicos que deben satisfacer todo sistema criptográfico analógico basado en caos, según Álvarez y Shujun (2006). Por ejemplo, se describen detalladamente los circuitos analógicos de encriptamiento y desencriptamiento, se implementan fácilmente para ser seguros, de bajo costo y rápidos en su respuesta, la llave de encriptamiento se debe definir por las señales caóticas sincronizadoras correspondientes (i.e., Vx2 y V'x2) finalmente, el espectro de la señal de información debe estar contenido completamente dentro de el de la señal caótica encriptadora (v.g., 0 a 6.25 KHz) y su magnitud (v.g., 50 a 100 mVp) debe ser varias veces menor que el de esta última (v.g., 300 hasta 700 mVp).

Definitivamente, la firma espectral de la señal caótica Vx2 (c.f., figura 18) marca el patrón de ocultamiento. Si se desea que el encriptamiento sea eficiente se requiere que la señal se mantenga dentro de la mascarilla establecida, por el alcance máximo en frecuencia (i.e., 6.25 KHz), y que su magnitud sea mayor a la del ruido de fondo y mucho menor a la de la caótica Vx2 (Núñez, 2006a y b). Si se desea ampliar la mascarilla, se necesita aumentar la dinámica caótica con circuitos hipercaóticos e incorporar procesos de convolución/correlación entre las señales caóticas y los mensajes.

Los resultados obtenidos se pueden mejorar utilizando componentes electrónicos de mayor grado, calidad y precisión. El circuito realizado y validado reafirma proponer un esquema de canales múltiples que lo hacen más eficiente, ya que así se cuenta con un canal bidirec-

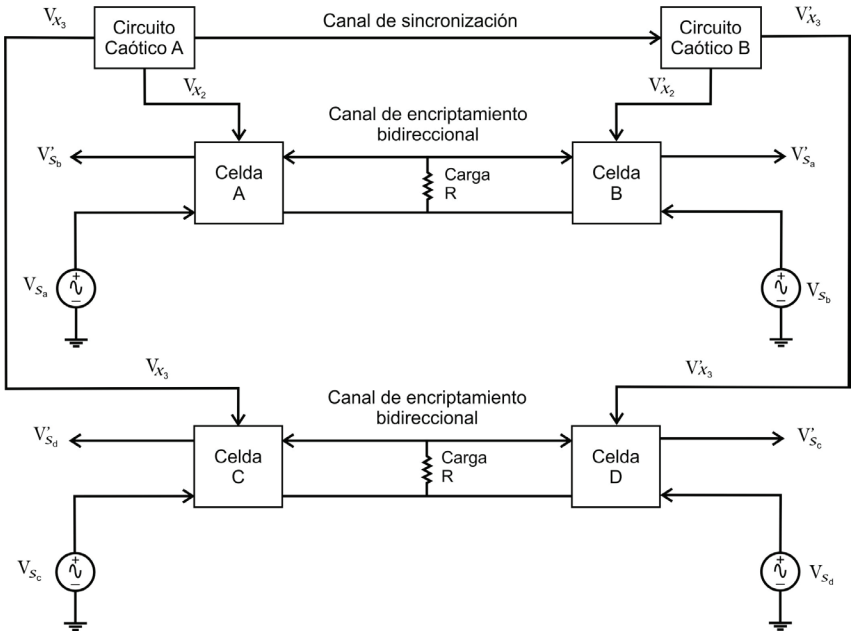


Figura 23. Diagrama a cuadros de la versión multicanal del circuito encriptador/desencriptador caótico bidireccional propuesto, con aplicación inmediata para los circuitos de Lorenz, Rössler y Chen, entre otros

cional más y es ideal para aplicarlo directamente a circuitos con dinámicas caóticas afines, de acuerdo con el utilizado en este estudio y por Lorenz, Rössler y Chen, entre otros. El esquema de canales múltiples que se propone se presenta en la figura 23, es una idea original y prometedora, ya que aumenta la rentabilidad (v.g., baja el índice costo/canal); en pocas palabras, aumenta a dos el número de canales bidireccionales por pareja de circuitos idénticos mencionados. Para lograr lo anterior, se requerían de 4 canales independientes. Una aplicación que se contempla es en las comunicaciones digitales de baja velocidad, para el envío bidireccional de mensajes binarios multiusuario utilizando modulación paramétrica. Es claro que se requiere estudiar más el comportamiento del circuito propuesto ante ruido eléctrico e inestabilidades propias de sus componentes para lograr mayor seguridad en el encriptamiento/desencriptamiento.

## Conclusiones

Se logró obtener un circuito encriptador/desencriptador bidireccional que utiliza un canal de corriente que lo hace ser rentable y confiable, cuando se construye por un par de circuitos idénticos de Chua sincronizados, según Carroll y Pecora. Se diseñó, probó y validó su funcionamiento tanto con el programa Workbench como experimentalmente en el laboratorio. Se presentan algunas simulaciones y experimentos comprobatorios del ocultamiento y recuperación propuestas, utilizando señales de referencia, de mediana frecuencia e incluyendo ruido eléctrico; los resultados fueron bastante semejantes y aceptables, además de ser calificados por los índices del factor de cresta y la distorsión armónica total. También, se puede mencionar que el circuito propuesto cumple con algunos requerimientos básicos que deben satisfacer todo sistema criptográfico analógico basado en caos según Álvarez y Shujun (2006).

Algo relevante que ofrece más certidumbre al procedimiento propuesto, es que la firma espectral de la señal caótica Vx2 marca el patrón de ocultamiento y si se desea que el encriptamiento sea eficiente, la señal de mensaje no debe salirse de la mascarilla establecida por los alcances aproximados de amplitud y frecuencia de 50 a 100 mVp y de 0.10 a 6.25 KHz, respectivamente. Si se desea ampliar la mascarilla de encriptamiento, se necesitan utilizar circuitos hipercaóticos y convolucionar o correlacionar, las señales caóticas con los mensajes en proceso.

Una de las principales bondades del encriptador/desencriptador por corriente propuesto es que puede utilizarse con cualquier pareja de circuitos caóticos idénticos, como los de Lorenz, de Chen, de Rössler, entre otros, en un esquema novedoso de canales múltiples. El esquema que se propone es original y prometedor, ya que aumenta la rentabilidad, en pocas palabras, aumenta a dos el número de canales bidireccionales por pareja de los circuitos idénticos mencionados. Para lograr lo anterior se requieren de 4 canales independientes.

Otra aplicación interesante es en el campo de las comunicaciones digitales de baja velocidad, se vislumbra una para el envío bidireccional de mensajes binarios multiusuario por medio de modulación paramétrica.

Se requiere estudiar más el comportamiento de los circuitos ante ruido eléctrico e inestabilidades de los componentes para aplicarlos confiablemente en el encriptamiento/desencriptamiento caótico bidireccional fuera del laboratorio.

## Agradecimientos

Agradecemos al CONACYT por apoyar económicamente el presente trabajo a través del proyecto: 7453, dirigido por el Dr. J. Álvarez G. y al Ing. A. Gutiérrez M.

## Referencias

Alvarez G., Shujun L. Some basic cryptographic requirements for chaos-based cryptosystems. *IJBC*, volumen 16 (número 8), 2006: 2129-2151.

Buscarino A., Fortuna L., Frasca M., Sciuto G. A concise guide to chaotic electronic circuits, *SpringerBriefs in Applied Sciences and Technology*, 2014.

Carroll T.L. y Pecora L.M. Synchronizing chaotic circuits. *IEEE Trans. on Circs. and Sys.*, volumen 38, 1991: 453-456.

Carroll T.L. y Pecora L.M. Synchronizing nonautonomous chaotic circuits. *IEEE Trans. Circs.*, volumen 40, 1993: 646-50.

Chua L.O., Kcarev L.J., Eckert K., Itoh M. Experimental chaos synchronization in Chua's circuits. *Int. J. Bifurc. Chaos*, volumen 2 (número 3), 1992: 705-708.

Chua L.O. A universal circuit for studying and generating chaos- part I/II: routes to chaos. *IEEE Trans. on circuits and systems*, volumen 40 (número 10), 1993: 732-744/745-762.

Corron N.J. y Hahs D.W. A new approach to communications using chaotic signals. *IEEE Trans. Circuits Systems I*, volumen 44 (número 5), 1997: 373-382.

Cruz C., López D., García V., Serrano H., Núñez R. Experimental realization of binary signal transmission using chaos. *JCSC*, volumen 14 (número 3), 2005: 453-468.

Cuomo K.M., Oppenheim A.V., Strogatz S.H. Synchronization of Lorenz-Based chaotic circuits with applications to communications. *IEEE Trans. on Circuits and Syst., II: Analog/ Digital and Signal Processing*, volumen 40 (número 10), 1993.

Cuomo K.M., Oppenheim A.V., Strogatz S.H. Robustness and signal recovery in a synchronized chaotic system. *IJBC*, volumen 3 (número 6), 1993: 1629-38.

Dedieu H., Kennedy M., Hasler M. Chaotic shift keying: Modulation and demodulation of a chaotic carrier using Chua's circuits.*IEEE Trans. Circts. Syst. II*, volumen 40 (número 10), 1993: 634-642.

Deng T., Guang-Qiong X., Liang-Ping C., Jian-Guo Ch.B., Xiao-Dong L., Zheng-Mao W. Bidirectional chaos synchronization and communication in semiconductors lasers with optoelectronic feedback. *Optics Communications*, volumen 282, 2009: 2243-2249.

Gámez L. y Cruz C. Synchronization of multi-scroll chaos generators: application to private communication. *Revista Mexicana de Fisica, FC-UNAM*, volumen 54 (número 4), 2008: 299-305.

Guang-Hui L., An-Bang W., Ye F., Yang W. Synchronization and bidirectional communication without delay line using strong mutually coupled semiconductor lasers. *Chin. Phys., B*, volumen 19 (número 7), 2010: 070515.

Hasler M. Synchronization principles and applications, en: Circuits and Systems Tutorials, C. Toumazou, NJ: IEEE, Ed. Piscataway, 1994, pp. 314-27.

Hasler M. y Schm T. Chaos communics. Over noisy channels. *IJBC*, volumen 10 (número 4), 2000: 719-35.

Kennedy M.P. Experimental chaos via Chua's circuit, en: Proc. of the 1st. Experimental Chaos Conference, editores Vohra S., Shlesinger M., Pecora M. L., Ditto W. 1992, pp. 340-51.

Kennedy M.P. Three steps to chaos-part I: evolution. *IEEE Trans. on circuits and systems*, volumen 40 (número 10), 1993: 640-656.

López D. y Crúz C. A note on chaos-based communication schemes. *Revista Mexicana de Física, FC-UNAM*, volumen 51 (número 3), 2005: 265-269.

Matsumoto T., Chua L.O., Komuro M. The doble scroll. *IEEE Trans. on Circs. and Sys.*, volume 32 (número 8), 1985: 797-818.

Milanovi'c V. y Zaghloul M.E. *Electronics Letters*, volumen 32 (número 1), 1996: 11.

Moon F.C. *Chaotic and fractal dynamics, an introduction for applied scientist and engineers*, W. & S., Inc., 758, 1992.

Núñez R. An optimal chaotic bidirectional communicator, based on synchronized Lorenz circuits, en: Procs. of 6th. Experimental Chaos Conference, 48, 22-6 julio, Potsdam, Germany, 2001.

Núñez R. Calificación experimental de la sincronía de dos circuitos caóticos, Congreso Internacional de la CLCA2004, La Habana, Cuba, 2004.

Núñez R. Comunicador experimental privado basado en encriptamiento caótico. *Revista Mexicana de Física*, FC-UNAM, volumen 52 (número 3), 2006a: 285-294.

Núñez R. Caracterización de un mensajero caótico binario con ruido en el canal: simulación y experimentación. *Revista Mexicana de Física, FC-UNAM*, volumen 52 (número 5), 2006b: 464-473.

Núñez R. Encriptador experimental retroalimentado de Lorenz con parámetros desiguales. *Revista Mexicana de Física, FC-UNAM*, volumen 52 (número 4), 2006: 372-378.

Núñez R. Measurement of Chua chaos and its applications. *JART, UNAM*, volumen 6 (número 1), 2008.

Núñez R. Spectrum richness as determinant of chaotic synchronization. *IEEELATIN A. TRANS.*, volumen 7 (número 5), 2009.

Núñez R. La tendencia del factor de cresta ayuda a detectar eventos nacientes; circuito electrónico, programas y aplicaciones a señales de diversas. *Ingeniería Investigación y Tecnología*, volumen XV (número 1), enero-marzo 2014: 63-81.

Núñez R. Sistema automático de pruebas LabVIEW7-PMD1208LS, Reporte técnico, DET-CICESE, 2008.

Parlitz U., Chua L.O., Kocarev L.J., Halle K.S., Shang A. Transmission of digital signals by chaotic synchronization. *IJBC*, volumen 2 (número 4), 1992: 973-77.

Pease R. *Analog circuits: world class designs*, Elsevier, Inc., 2008, p. 100.

Posadas C., Cruz C., Núñez R. Experimental realization of binary signal transmission based on Lorenz circuit. *JART*, volumen 2 (número 2), 2004: 127-36.

Sepúlveda A. *Diseño y realización de una fuente de corriente para aplicaciones en opto electrónica*, (tesis de maestría en ciencias), DET-CICESE, 2010.

Varrientos J., Sánchez E., Rodríguez A. A current-mode synchronous chaotic circuit for signal encryption, 0-7803-2428-5/95. *IEEE Trans. Circ. and Sys.*, 1995: 133-37.

Shun-Chuan T., Chuan-Kuei H., Dong-Liang Q., Wan-Tai Ch. Implementation of bidirectional chaotic communication systems based on Lorenz circuits. *Chaos, Solitons and Fractals*, volumen 20, 2004: 567-579.

Yongguang Y. The synchronization for time-delay of linearly bidirectional coupled chaotic system. *Chaos, Solitons and Fractals*, volumen 33, 2007: 1197-1203.

Wagemakers A., Buldu J.M., Sanjuan M.A.F. Experimental demonstration of bidireccional chaotic communication by means of isochronal synchronization. *EPL*, volumen 81, 2008, p. 4005.

**Citación sugerida**

**Citación estilo Chicago**

Núñez-Pérez, Ricardo Francisco. Fuentes de corriente reducen a un canal la comunicación por encriptamiento caótico bidireccional. *Ingeniería Investigación y Tecnología*, XVIII, 04 (2017): 353-368.

**Citación estilo ISO 690**

Núñez-Pérez R.F. Fuentes de corriente reducen a un canal la comunicación por encriptamiento caótico bidireccional. *Ingeniería Investigación y Tecnología*, volumen XVIII (número 4), octubre-diciembre 2017: 353-368.

## Semblanza del autor

*Ricardo Francisco Núñez-Pérez.* M. en C. en instrumentación electrónica (1987), CICESE, México. Licenciado en ingeniería electrónica (1980) por la UABC, México con mención honorífica en ambos grados. Desde 1987 a la fecha es profesor/investigador en el Departamento de Electrónica y Telecomunicaciones del Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE). Recibió el primer lugar con su tesis de maestría en el IV Certamen Nacional sobre diseño de Equipo Electrónico Aplicado al Sector Eléctrico, organizado por el IIE, CONACYT, SEP y la CFE (1988), así también el 1er. lugar y la Presea en Ciencias y Tecnología en el IV Certamen Nacional del CREA, área electrónica (1988). Recibió un reconocimiento por dirigir la tesis de licenciatura ganadora del 1er. lugar en el VI Certamen Nacional sobre Diseño de Equipo Electrónico Aplicado al Sector Eléctrico, organizado por el IIE, CONACYT, SEP y CFE (1990), perteneció al SNI de 1988 a 1993. Sus áreas de investigación e instrucción son: Desarrollo competitivo de instrumentación y equipo electrónico científico e industrial, realización de estudios de circuitos caóticos y sus aplicaciones y utilización práctica de los PDS en el análisis, síntesis y control digital de señales caóticas, biomédicas y de vibración mecánica (cuidado de maquinaria), entre otras.