DESDE 2013
https://repository.uaeh.edu.mx/revistas/index.php/icbi/issue/archive
Pädi Boletín Científico de Ciencias Básicas e Ingenierías del ICBI
ISSN: 2007-6363

Publicación Semestral Pädi Vol. 11 No. Especial 2 (2023) 167-174

Emulación en FPGA de un Esquema de Modulación Caótica CSK con Portadoras Reconfigurables
FPGA Emulation of Reconfigurable Carrier CSK Chaotic Modulation Scheme

J.C. Núñez-Pérez[a,*], M.A. Estudillo-Valdez[a], A. Calvillo-Téllez[a]

[a]*Instituto Politécnico Nacional, IPN-CITEDI, Tijuana, Baja California, México.*

Resumen

En este artículo se presenta una arquitectura para un transmisor-receptor con modulación caótica CSK y sincronización hamiltoniana. Las portadoras utilizadas se generaron utilizando un oscilador que imita el comportamiento de múltiples osciladores caóticos. Para este caso se generaron 6 osciladores caóticos, 3 de ellos en tres dimensiones (3D) y los otros 3 en cuatro dimensiones (4D). La arquitectura fue diseñada para una tarjeta FPGA Artix7-AC701 con chip xc7a200tfbg676. La aritmética binaria es de 32 bits, 1 bit para el signo, 21 para la parte entera y 10 para la parte fraccionaria. Por otro lado, el método numérico implementado a fin de no superar los recursos lógicos del chip FPGA fue el de punto medio, con el cual se consiguió generar las formas de onda de diversos osciladores caóticos sin divergencia en las trayectorias. La principal contribución de esta investigación es una metodología de sincronización con portadoras variables en el tiempo, cada variación corresponde a un oscilador distinto ya sea tridimensional o en hiperplano.

Palabras Clave: caos, CSK, FPGA, modulación, VHDL.

Abstract

This article introduces the architecture of a transmitter-receiver system that employs chaotic CSK modulation and Hamiltonian synchronization. To generate the carriers, an oscillator was utilized, which emulates the behavior of multiple chaotic oscillators. In this particular case, six chaotic oscillators were generated, with three operating in three dimensions (3D) and the other three in four dimensions (4D). The architecture was implemented on an Artix7-AC701 FPGA board featuring the xc7a200tfbg676 chip. Binary arithmetic with a precision of 32 bits was employed, with 1 bit assigned for the sign, 21 for the integer part, and 10 for the fractional part. To avoid exceeding the logical resources of the FPGA chip, the midpoint method was implemented. This method ensures that the generated chaotic oscillators do not diverge in their trajectories. The primary contribution of this study is a synchronization method for variables, where each variation corresponds to a different oscillator, either in the three-dimensional or hyperplane domain.

Keywords: chaos, CSK, FPGA, modulation, VHDL.

1. Introducción

Actualmente existen esquemas de comunicación que permiten realizar transmisiones que le proporcionan a la información confidencialidad y la mantienen integra durante una transmisión. Sin embargo, de acuerdo con (Xu, 2022) los esquemas de comunicación basados en caos tienen en general menores probabilidades de ser descifrados en comparación con esquemas convencionales. Tal como se menciona en (Xu, 2022), ya se han establecido métricas para verificar la resistencia de un método ante ataques diferenciales o por fuerza bruta.

El manejo de datos masivos ha llevado a explorar alternativas con mejor desempeño y menor probabilidad de descifrado utilizando esquemas caóticos sincronizados y no sincronizados. En (Xu, 2016) y (Posadas, 2014) se utilizan sistemas sincronizados en donde el sistema transmisor tiene un oscilador caótico maestro generando las señales portadoras del mensaje; después se transmiten al receptor, el cual contiene un oscilador caótico idéntico llamado observador que se sincroniza con el sistema maestro para recuperar la información. Por otro lado, en (Kaddoum, 2017) se utiliza un sistema de comunicación no sincronizado, este tipo de

*Autor para la correspondencia: nunez@citedi.mx
Correo electrónico: nunez@citedi.mx (José Cruz Núñez-Pérez), mestudillo@citedi.mx (Miguel Angel Estudillo-Valdez), calvillo@citedi.mx (Andrés Calvillo-Téllez).

Historial del manuscrito: recibido el 27/03/2023, última versión-revisada recibida el 01/06/2023, aceptado el 28/06/2023, publicado el 11/09/2023. **DOI:** https://doi.org/10.29057/icbi.v11iEspecial2.10849

comunicaciones posee una señal modulada que contiene la información necesaria para recuperar el mensaje transmitido.

En otras investigaciones, como en (Rezk, 2019) se han desarrollado sistemas que encriptan la información antes de la modulación, en este caso se implementó la posibilidad de utilizar dos o tres osciladores caóticos implementados en una misma tarjeta FPGA. Lo anterior con el fin de realizar múltiples encriptaciones a la información, la desventaja de implementar múltiples osciladores caóticos es que requieren más recursos lógicos. En (Liu, 2002) se encontraron los parámetros adecuados para cambiar de un oscilador caótico a otro utilizando el mismo sistema de ecuaciones, lo que reduce significativamente el requerimiento de recursos lógicos de la arquitectura.

En esta investigación se propone una técnica de modulación caótica basada en sincronización Hamiltoniana, se utilizan como sistema maestro y esclavo un oscilador reconfigurable de 4 canales. Este oscilador pasa del régimen de un oscilador caótico a otro durante un mismo proceso de transmisión. Cabe mencionar que este generador de caos puede generar formas de onda 3D y 4D. La simulación se realiza sobre un tren de pulsos en binario con encriptación X-OR previo a la modulación. Las portadoras caóticas que pueden variar indefinidamente a intervalos regulares establecidos por el usuario, emulando formas de onda de osciladores como el de Qi, cuatro alas, Qiang, Leilei, Lorenz, Newton-Leipnik, entre otros (Zhang, 2012), (Hu, 2013), (Qi, 2006), (Effati, 2014), (Zhou, 2016), (Abedini, 2014), (Lai, 2018).

2. Marco Teórico

2.1. Osciladores Caóticos

Uno de los osciladores caóticos más populares de la literatura fue descubierto accidentalmente durante unos experimentos en el año de 1963 por el meteorólogo Edward Norton Lorenz. A partir de entonces se han estudiado con más énfasis y se han implementado en diversas aplicaciones o para dar explicación a fenómenos inexplicables con sistemas caóticos.

Algunas de sus características relevantes para esta investigación es que son: (1) deterministas, es decir, pueden ser representados mediante modelos matemáticos, por tanto, no son modelos aleatorios; (2) poseen sensibilidad a las perturbaciones, ya sea en condiciones iniciales o durante la evolución del oscilador, la más mínima modificación altera el comportamiento del oscilador exponencialmente; (3) son prácticamente impredecibles si no se conocen los aspectos de su configuración, tales como el método numérico, parámetros de control, condiciones iniciales, condiciones de punto fijo o punto flotante, tamaño de paso y longitud de palabra; y finalmente (4) tienen baja autocorrelación, es decir un segmento de señal caótica difiere en sus formas de onda respecto de segmentos de la misma longitud y de la misma señal en diferentes fases de tiempo.

En la Tabla 1 se muestran las ecuaciones de los osciladores caóticos 3D utilizados en esta investigación (Qi, 2015), (Wang, 2019), (Wang, 2010).

Tabla 1: Osciladores caóticos tridimensionales.

Oscilador caótico	Sistema de Ecuaciones	Parámetros
Lorenz	$\begin{cases}\dot{x} = a(y-x)\\ \dot{y} = rx - y - xz\\ \dot{z} = xy - bz\end{cases}$	$a = 16, r = 45,$ $b = 4$
Cuatro alas	$\begin{cases}\dot{x} = a(y-x) + eyz\\ \dot{y} = cx + dy - xz\\ \dot{z} = xy - bz\end{cases}$	$a = 14, b = 43,$ $c = -1, d = 16,$ $e = 4$
Chen-Lee	$\begin{cases}\dot{x} = ax - yz\\ \dot{y} = by + xz\\ \dot{z} = cz + dxy\end{cases}$	$a = 5, b = -10$ $c = -0.38, d = 0.33$

Mientras que en la Figura 1 se muestran las formas de onda de los osciladores de la Tabla 1 en sus planos *x-y-z*.

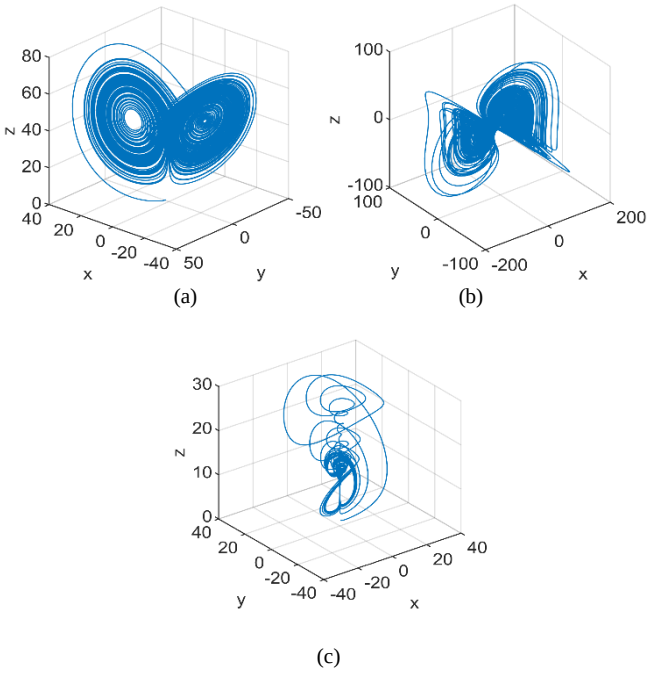


Figura 1: Osciladores caóticos (a) Lorenz, (b) Cuatro alas, (c) Chen-Lee.

Por otro lado, en la Tabla 2 se muestran 3 conjuntos de ecuaciones para la generación de osciladores en 4D y sus parámetros (Zhang, 2018).

Tabla 2: Osciladores caóticos en hiperplano.

Oscilador caótico	Sistema de Ecuaciones	Parámetros
Dadras	$\begin{cases}\dot{w} = aw + by\\ \dot{x} = cx - yz\\ \dot{y} = xz + dy\\ \dot{z} = exy + fz + gxw\end{cases}$	$a = 0.05,$ $b = -0.2, c = 8,$ $d = -43.75,$ $e = 2, f = -10,$ $g = 5$
Leilei	$\begin{cases}\dot{w} = ax + byz\\ \dot{x} = c(y-x)\\ \dot{y} = dx - y - xz + w\\ \dot{z} = xy - ez\end{cases}$	$a = 8, b = 0.1,$ $c = 10, d = 20,$ $e = 8/3$
Liu	$\begin{cases}\dot{w} = ax + byz\\ \dot{x} = c(y-x)\\ \dot{y} = dx - y - xz + w\\ \dot{z} = xy + ez + ywx\end{cases}$	$a = 8, b = 0.1,$ $c = 10, d = 20,$ $e = 8/3$

En la Figura 2 se muestran las formas de onda de los osciladores de la Tabla 2 en sus diferentes vistas.

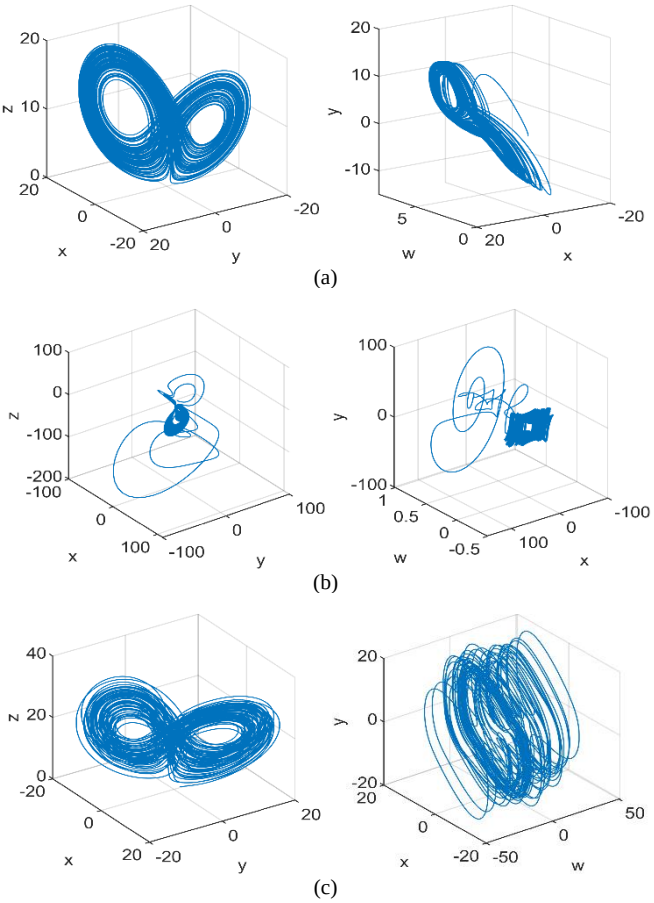


Figura 2: Osciladores en 4 dimensiones (a) Liu 4D, (b) Dadras, (c) Leilei.

Para fines prácticos las condiciones iniciales de los osciladores en las Tablas 1 y 2 se establecieron en 1 para todas las ecuaciones de estado.

3. Esquema CSK

Una modulación digital caótica CSK requiere de un proceso de sincronización entre transmisor y receptor. Su funcionamiento se basa en una inversión horizontal en la señal portadora dependiendo del estado del bit del mensaje b∈{-1,+1}. En la Figura 3 se muestra el diagrama de su funcionamiento.

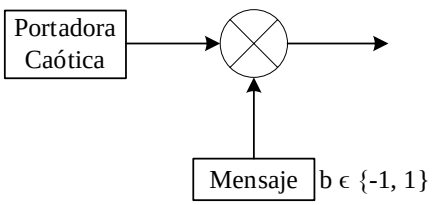


Figura 3: Diagrama de una modulación CSK.

La Figura 4(a) muestra un canal de un oscilador caótico, la Figura 4(b) muestra el mensaje en binario 101001010011, esta señal también es conocida como señal moduladora, y la Figura 4(c) muestra la señal modulada, las porciones en rojo corresponden con los bit bajo o cero, mientras que los bits altos o uno se muestran de color azul.

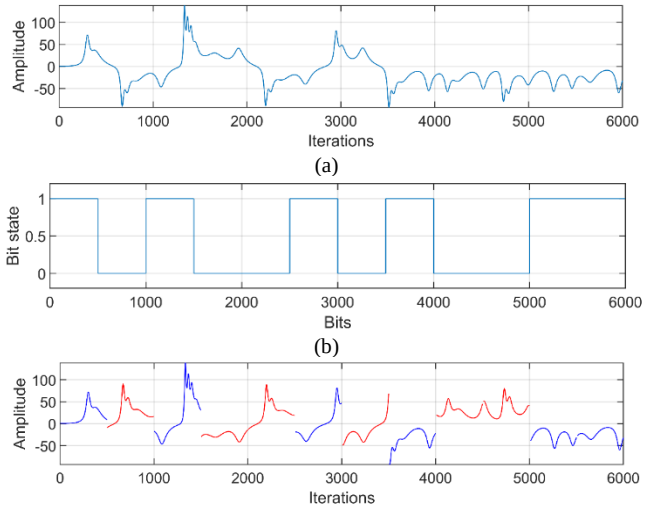


Figura 4: Señales de una modulación CSK, (a) portadora, (b) mensaje y (c) señal modulada.

4. Sincronización Hamiltoniana

En esta sección es utilizado el oscilador de cuatro alas de la Tabla 1 para desarrollar las ecuaciones que permiten una sincronización Hamiltoniana,

$$\left.\begin{aligned} \dot{x} &= ax + by + cyz \\ \dot{y} &= dy - xz \\ \dot{z} &= ez + fxy \end{aligned}\right\}, \qquad (1)$$

en donde (a, b, c, d, e, f) son los parámetros de control y (x, y, z) son las variables de estado. Se considera el sistema no lineal en la forma Hamiltoniana Generalizada de la ecuación (2),

$$\dot{x} = J(x)\frac{\partial \boldsymbol{H}}{\partial x} + S(x)\frac{\partial \boldsymbol{H}}{\partial x}, \qquad x \in \mathbb{R}^n \qquad (2)$$

en donde **H**(x) describe una función de energía que está definida globalmente positiva. El vector gradiente de **H** se denota con $\partial \mathbf{H}/\partial x$ y se utiliza una función de energía de la forma $\mathbf{H}(x) = (1/2)x^{T}Mx$. Además, las matrices cuadradas J(x) y S(x) satisfacen $J(x) + J^{T}(x) = 0$ y $S(x) = S^{T}(x)$. Por otro lado, si se considera una clase especial de sistemas hamiltonianos generalizados con campos vectoriales desestabilizadores, se obtiene la ecuación (3),

$$\left.\begin{aligned} \dot{x}_m &= J(y)\frac{\partial \boldsymbol{H}}{\partial x_m} + (I + S)\frac{\partial \boldsymbol{H}}{\partial x_m} + \boldsymbol{F}(y), \qquad x_m \in \mathbb{R}^n \\ y &= C\frac{\partial \boldsymbol{H}}{\partial x_m}, \qquad y \in \mathbb{R}^n \end{aligned}\right\}, \qquad (3)$$

en donde C corresponde con una matriz constante, I es una matriz simétrica diagonal constante y $\boldsymbol{F}$ corresponde con una función independiente y que forma parte del oscilador caótico. Al seleccionar las variables x_e y η como vector de estado y estimados, respectivamente, a la salida se genera un sistema

observador a partir de la ecuación (3) representado por la ecuación (4) con un vector K conocido como el vector ganancia del observador,

$$\begin{aligned} \dot{x}_e &= J(y)\frac{\partial \boldsymbol{H}}{\partial x_e} + (I+S)\frac{\partial \boldsymbol{H}}{\partial x_e} + \boldsymbol{F}(y) + K(y-\eta) \\ \eta &= C\frac{\partial \boldsymbol{H}}{\partial x_e} \end{aligned}, \quad (4)$$

A partir de la ecuación (3) y (4) se puede desarrollar el proceso de sincronización de manera estructurada como se presenta a continuación.

- Primero se obtiene la función de energía seleccionando la función de energía cuadrática mostrada en la ecuación (5),

$$\boldsymbol{H}(x) = \frac{1}{2}[ax^2 + by^2 + z^2], \quad (5)$$

a su vez el vector gradiente de la ecuación (5) se muestra en la ecuación (6),

$$\frac{\partial \boldsymbol{H}}{\partial x} = \begin{bmatrix} ax \\ by \\ z \end{bmatrix} = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \boldsymbol{P}\boldsymbol{x}. \quad (6)$$

En donde $\boldsymbol{x}$ corresponde con el vector de variables del oscilador.

- Segundo se obtienen las matrices J y S, estas se obtienen mediante la representación matricial del oscilador caótico modelado mediante la ecuación (1), y resultando la ecuación (7),

$$Ax = \begin{bmatrix} a & b & cy \\ 0 & d & -x \\ fy & 0 & e \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix}. \quad (7)$$

La ecuación (7) se reescribe en términos de J y S generando la ecuación (8),

$$A = \boldsymbol{R}\frac{\partial \boldsymbol{H}}{\partial x} = [J(y) + S(y)]\frac{\partial \boldsymbol{H}}{\partial x}, \quad (8)$$

en donde R es una matriz auxiliar, y que al ser despejada toma la forma de la ecuación (9),

$$\boldsymbol{R} = \boldsymbol{A}\boldsymbol{P}^{-\boldsymbol{1}} = \begin{bmatrix} 1 & 1 & cy \\ 0 & d/b & -x \\ fy/a & 0 & e \end{bmatrix}, \quad (9)$$

a partir de la ecuación (9) se pueden obtener las siguientes relaciones:

$$S(x) = \frac{1}{2}(R + R^T) = \begin{bmatrix} 1 & \frac{1}{2} & \frac{cy}{2} + \frac{fy}{2a} \\ \frac{1}{2} & \frac{d}{b} & -\frac{x}{2} \\ \frac{cy}{2} + \frac{fy}{2a} & -\frac{x}{2} & e \end{bmatrix}, \quad (10)$$

$$J(x) = \frac{1}{2}(R - R^T) = \begin{bmatrix} 0 & \frac{1}{2} & \frac{cy}{2} - \frac{fy}{2a} \\ -\frac{1}{2} & 0 & -\frac{x}{2} \\ \frac{fy}{2a} - \frac{cy}{2} & \frac{x}{2} & 0 \end{bmatrix}, \quad (11)$$

para este caso se considera la matriz C como se muestra en la ecuación (12),

$$C = [1\ 0\ 0]. \quad (12)$$

- Tercero se realiza la sincronización del sistema maestro observador, el sistema maestro se obtiene a partir de desarrollar la ecuación (3) como se muestra en la ecuación (13)

$$\begin{bmatrix} \dot{x}_m \\ \dot{y}_m \\ \dot{z}_m \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{2} & \frac{cy}{2} - \frac{fy}{2a} \\ -\frac{1}{2} & 0 & -\frac{x}{2} \\ \frac{fy}{2a} - \frac{cy}{2} & \frac{x}{2} & 0 \end{bmatrix}\begin{bmatrix} ax \\ by \\ z \end{bmatrix} + \begin{bmatrix} 1 & \frac{1}{2} & \frac{cy}{2} + \frac{fy}{2a} \\ \frac{1}{2} & \frac{d}{b} & -\frac{x}{2} \\ \frac{cy}{2} + \frac{fy}{2a} & -\frac{x}{2} & e \end{bmatrix}\begin{bmatrix} ax \\ by \\ z \end{bmatrix}, \quad (13)$$

de la ecuación (13) se desarrollan las multiplicaciones y se obtiene la ecuación (14)

$$\begin{bmatrix} \dot{x}_m \\ \dot{y}_m \\ \dot{z}_m \end{bmatrix} = \begin{bmatrix} \frac{by}{2} + \frac{cyz}{2} - \frac{fyz}{2a} \\ -\frac{ax}{2} - \frac{xz}{2} \\ \frac{fyax}{2a} - \frac{cyax}{2} + \frac{byx}{2} \end{bmatrix} + \begin{bmatrix} ax + \frac{by}{2} + \frac{cyz}{2} + \frac{fyz}{2a} \\ \frac{ax}{2} + \frac{byd}{b} - \frac{xz}{2} \\ \frac{cyax}{2} + \frac{fyax}{2a} - \frac{byx}{2} + ez \end{bmatrix}, \quad (14)$$

si las matrices de la ecuación (14) se suman resulta la ecuación (15), que corresponde con el sistema de ecuaciones del oscilador de cuatro alas original,

$$\begin{bmatrix} \dot{x}_{m1} \\ \dot{y}_{m1} \\ \dot{z}_{m1} \end{bmatrix} = \begin{bmatrix} ax + by + cyz \\ yd - xz \\ fyx + ez \end{bmatrix}. \quad (15)$$

Del mismo modo, el sistema observador queda representado a partir de desarrollar la ecuación (4) como se muestra en la ecuación (16),

$$\begin{bmatrix} \dot{x}_e \\ \dot{y}_e \\ \dot{z}_e \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{2} & \frac{cy}{2} - \frac{fy}{2a} \\ -\frac{1}{2} & 0 & -\frac{x}{2} \\ \frac{fy}{2a} - \frac{cy}{2} & \frac{x}{2} & 0 \end{bmatrix}\begin{bmatrix} ax \\ by \\ z \end{bmatrix}$$

$$+\begin{bmatrix} 1 & \frac{1}{2} & \frac{cy}{2}+\frac{fy}{2a} \\ \frac{1}{2} & \frac{d}{b} & -\frac{x}{2} \\ \frac{cy}{2}+\frac{fy}{2a} & -\frac{x}{2} & e \end{bmatrix}\begin{bmatrix} ax \\ by \\ z \end{bmatrix}+\begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix}(y-\eta), \quad (16)$$

en donde η es representado mediante la ecuación (17),

$$\eta = C\frac{\partial H}{\partial \xi}. \quad (17)$$

Al multiplicar las matrices de la ecuación (16) se obtiene

$$\begin{bmatrix} \dot{x}_e \\ \dot{y}_e \\ \dot{z}_e \end{bmatrix}=\begin{bmatrix} \frac{by}{2}+\frac{cyz}{2}-\frac{fyz}{2a} \\ -\frac{ax}{2}-\frac{xz}{2} \\ \frac{fyax}{2a}-\frac{cyax}{2}+\frac{byx}{2} \end{bmatrix}+\begin{bmatrix} ax+\frac{by}{2}+\frac{cyz}{2}+\frac{fyz}{2a} \\ \frac{ax}{2}+\frac{byd}{b}-\frac{xz}{2} \\ \frac{cyax}{2}+\frac{fyax}{2a}-\frac{byx}{2}+ez \end{bmatrix}$$
$$+\begin{bmatrix} k_1(x_m-x_e) \\ k_2(y_m-y_e) \\ k_3(z_m-z_e) \end{bmatrix}, \quad (18)$$

finalmente, al sumar las matrices de la ecuación (18) se obtiene el sistema observador compacto

$$\begin{bmatrix} \dot{x}_{e1} \\ \dot{y}_{e1} \\ \dot{z}_{e1} \end{bmatrix}=\begin{bmatrix} ax+by+cyz+k_1(x_{m1}-x_{e1}) \\ yd-xz+k_2(y_{m1}-y_{e1}) \\ fyx+ez+k_3(z_{m1}-z_{e1}) \end{bmatrix}. \quad (19)$$

5. Oscilador Reconfigurable

El oscilador reconfigurable, utilizado tanto en el transmisor como en el receptor, tiene la forma de la ecuación (20),

$$\dot{\boldsymbol{V}} = \boldsymbol{P}\cdot\boldsymbol{v} \quad (20)$$

en donde $\dot{\boldsymbol{V}}$ corresponde con las ecuaciones de estado, $\boldsymbol{P}$ representa la matriz de coeficientes o parámetros del sistema y $\boldsymbol{v}$ es igual al vector de variables. En las ecuaciones (21)-(23) se presentan las componentes de la ecuación (20),

$$\dot{\boldsymbol{V}} = [\dot{\boldsymbol{w}} \quad \dot{\boldsymbol{x}} \quad \dot{\boldsymbol{y}} \quad \dot{\boldsymbol{z}}]^T, \quad (21)$$

$$\boldsymbol{P}=\begin{bmatrix} \frac{p_{11}}{w} \\ \frac{p_{21}}{x} \\ \frac{p_{31}}{y} \\ \frac{p_{41}}{z} \end{bmatrix}+\begin{bmatrix} p_{12} & p_{13} & p_{14} & p_{15} \\ p_{22} & p_{23} & p_{24} & p_{25} \\ p_{32} & p_{33} & p_{34} & p_{35} \\ p_{42} & p_{43} & p_{44} & p_{45} \end{bmatrix}$$

$$+\begin{bmatrix} p_{16}xy/w & p_{17}z & p_{18}xw/y & p_{19}y \\ p_{26}xy/w & p_{27}z & p_{28}xw/y & p_{29}y \\ p_{36}xy/w & p_{37}z & p_{38}xw/y & p_{39}y \\ p_{46}xy/w & p_{47}z & p_{48}xw/y & p_{49}y \end{bmatrix}, \quad (22)$$

$$\boldsymbol{v} = [w \;\; x \;\; y \;\; z]^T. \quad (23)$$

El sistema de la ecuación (20) se puede adaptar para generar los osciladores de Newton-Leipnik, Chen, Rossler, cuatro alas, Lorenz, Qi, Leilei, Qiang, Sakaraya, Liu, entre otros.

5.1. Sincronización Hamiltoniana para un oscilador reconfigurable 4D

A partir de la metodología planteada para la sincronización Hamiltoniana y utilizando el oscilador reconfigurable de la ecuación (20), el oscilador maestro se puede establecer como sigue

$$\dot{\boldsymbol{V}}_{\boldsymbol{m}} = \boldsymbol{P}\cdot\boldsymbol{v} \quad (24)$$

en donde $\dot{\boldsymbol{V}}_m$ corresponde con las ecuaciones de estado del oscilador reconfigurable maestro, $\boldsymbol{P}$ representa la matriz de coeficientes o parámetros del sistema maestro y $\boldsymbol{v}$ es igual al vector de variables. Estas últimas dos ecuaciones tienen las mismas variables que el sistema presentado por la ecuación (25). Mientras que el oscilador reconfigurable esclavo se presenta como,

$$\dot{\boldsymbol{V}}_{\boldsymbol{e}} = \boldsymbol{P}\cdot\boldsymbol{v} + \boldsymbol{K}\cdot\boldsymbol{\varepsilon} \quad (25)$$

en donde $\dot{\boldsymbol{V}}_e$ son las ecuaciones de estado del oscilador reconfigurable esclavo, $\boldsymbol{P}$ representa la matriz de coeficientes del sistema esclavo, $\boldsymbol{v}$ es el vector de variables, $\boldsymbol{K}$ corresponde con el vector de ganancias del sistema de sincronización y $\boldsymbol{\varepsilon}$ equivale a los errores de sincronización entre el maestro y el esclavo, tal como muestran las ecuaciones (26) y (27),

$$\boldsymbol{K} = [k_1 \; k_2 \; k_3 \; k_4]^T, \quad (26)$$

$$\boldsymbol{\varepsilon} = [(w_m-w_e),(x_m-x_e),(y_m-y_e),(z_m-z_e)]^T, \quad (27)$$

donde $\boldsymbol{P}$ y $\boldsymbol{v}$ tienen las mismas variables que el sistema presentado por la ecuación (20).

6. Arquitectura en VHDL

6.1. Sincronización

El circuito de sincronización consiste en los cuatro elementos mostrados en la Figura 5. El elemento *control_caos* cambia a intervalos regulares los parámetros del oscilador, en este módulo pueden ir configurados una cantidad arbitraria de osciladores, en este caso se han configurado 6. El módulo *Tx* corresponde a la transmisión, este inicia la generación de los cuatro canales del oscilador indicado por el módulo *control_caos*. El módulo *Rx* es de recepción, este inicia con el mismo oscilador caótico y parámetros que el módulo de transmisión, pero con diferentes condiciones iniciales. Las salidas de los módulos de transmisión y recepción entran en el módulo *error_sinc*, este calcula las diferencias entre los canales y aplica la ganancia de sincronización correspondiente de cada canal. A la salida de este módulo se generan cuatro señales de corrección de trayectoria, que a su vez entran en el módulo de recepción para corregir las formas de onda. Al cabo

de las iteraciones el transmisor y receptor quedan completamente sincronizados.

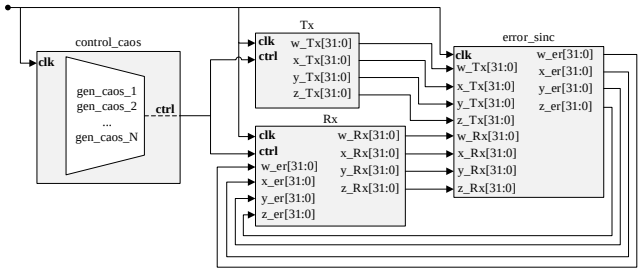


Figura 5: Diagrama del circuito de sincronización y corrección de error.

6.2. Encriptación y Modulación CSK

En esta sección se tienen tres subsecciones principales mostradas en la Figura 6, el bloque Señales Pseudo-Aleatorias (SPA) recibe los canales del oscilador maestro y genera las secuencias pseudoaleatorias. En el bloque de encriptación se enmascaran los canales de mensaje utilizando las secuencias pseudoaleatorias del bloque SPA y un operador lógico X-OR. Las señales encriptadas se utilizan como moduladoras en el bloque de *Modulación CSK*.

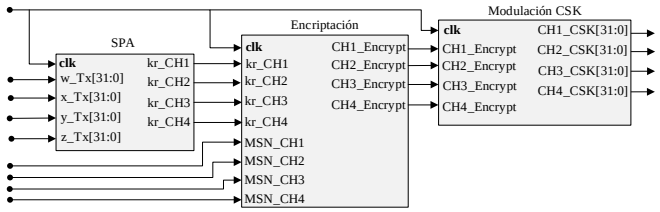


Figura 6: Circuito de encriptación y modulación mediante CSK.

6.3. Desencriptación y Demodulación CSK

Esta sección consta de tres segmentos principales mostrados en la Figura 7, el demodulador interpreta los bits a partir de la modulación CSK del transmisor. Por otro lado, el bloque SPA, que se encuentra sincronizado con el oscilador del transmisor y realiza los mismos cambios de oscilador, genera las mismas secuencias que en el transmisor.

Finalmente, el módulo de desencriptación opera las secuencias pseudoaleatorias y los bits del demodulador para desencriptarlos mediante una operación X-OR. Las señales resultantes corresponden con las del mensaje original llamadas como *MSN_CH1*, *MSN_CH2*, *MSN_CH3*, *MSN_CH4*.

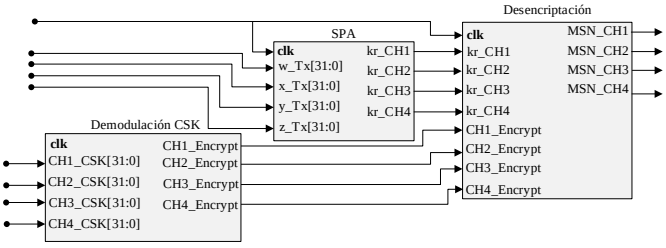


Figura 7: Diagrama a bloques para una demodulación y desencriptación.

7. Simulación de sincronización Hamiltoniana

En la Figura 8 se muestran los seis segmentos principales de la portadora caótica para el canal “x”. Siendo (1) oscilador caótico de cuatro alas, (2) oscilador de Lorenz en 3D, (3) oscilador de Chen-Lee en 3D, (4) oscilador de Dadras en 4D, (5) Oscilador de Leilei en 4D y (6) oscilador de Liu en 4D.

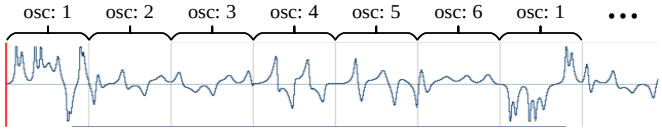


Figura 8: Portadora caótica generada con 6 osciladores distintos.

La sincronización se mantiene activa durante todo el proceso de transmisión y corrige irregularidades durante los cambios de oscilador. Sin embargo, al cabo de 50 μs el sistema queda completamente sincronizado, en la Figura 9 se muestran los primeros 25 μs de sincronización en donde *error_CH1* el error durante la sincronización del canal, “w” del transmisor y receptor, *error_CH2* canal “x”, *error_CH3* canal “y” y *error_CH4* canal “z”.

Figura 9: Errores de sincronización al inicio de la simulación.

8. Resultados

En la Figura 10 se muestran las señales básicas para encriptación y modulación mediante CSK, *chaos_x_Tx* corresponde con el canal del oscilador. De esta señal y mediante un muestreo regular de la amplitud del canal se obtiene la señal pseudoaleatoria *spa_Tx_CH2*, *MSN_CH2* es el tren de pulsos de mensaje, las señales *spa_Tx_CH2* y *MSN_CH2* se operan mediante X-OR para obtener la señal mensaje encriptada, la señal *Kry_Tx_CH2* corresponde con el tren de pulsos encriptados. Además, funciona como moduladora utilizando como portadora el canal del oscilador reconfigurable. Finalmente, la señal CSK_CH2 es la señal modulada. Del mismo modo se procesan los canales *w*, *y*, *z*.

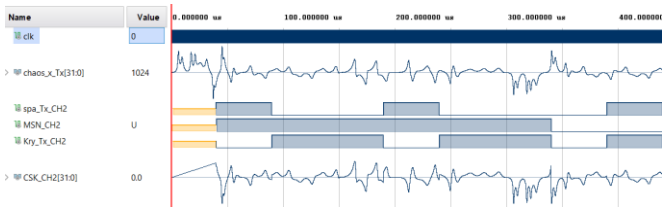


Figura 10: Señales para encriptar y modular mediante CSK.

Por otro lado, en la Figura 11 se muestran las señales para demodulación y desencriptación del canal "*x*", *CSK_CH2* corresponde con la señal modulada capturada en el receptor, *chaos_x_Rx* es el canal del oscilador sincronizado. A partir de esta señal se crea la señal pseudoaleatoria *spa_Rx_CH2*, mientras que la señal *Kry_Rx_CH2* son los bits recuperados de la demodulación. Después de operar las señales *Kry_Rx_CH2* y *spa_Rx_CH2* mediante X-OR se obtiene la señal de mensaje original *Dekry_Rx_CH2*.

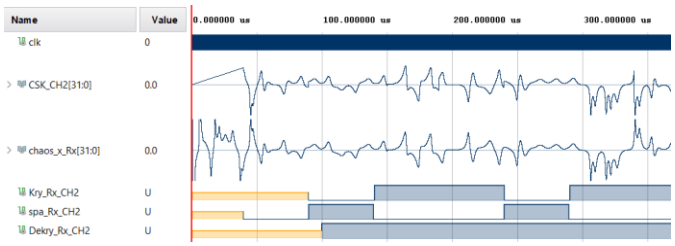
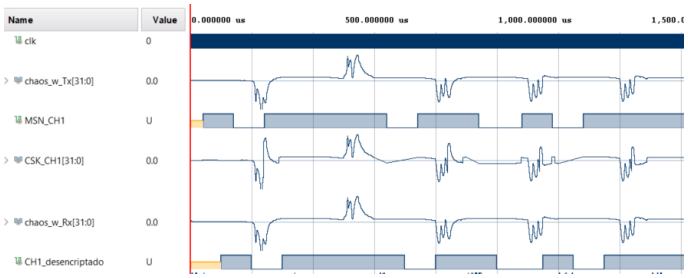
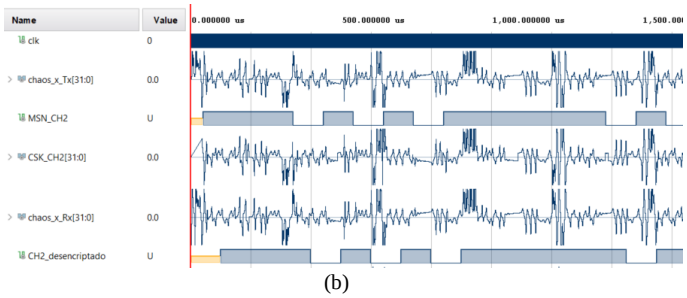


Figura 11: Demodulación y desencriptación CSK.

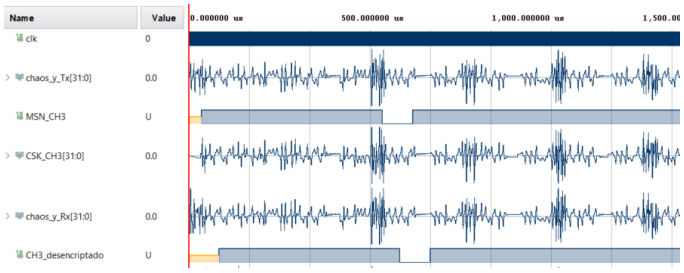
En la Figura 12 se muestra la simulación de los cuatro canales de comunicación utilizando la técnica de modulación digital caótica CSK, tomando como portadora diferentes señales caóticas. *Chaos_w_Tx* corresponde con el canal "*w*" del oscilador caótico, *MSN_CH1* es la representación digital del mensaje, *CSK_CH1* representa la modulación del canal 1 de comunicación utilizando como portadora la señal *Chaos_w_Tx*. Finalmente, la señal *CH1_desencriptado* corresponde con el mensaje recuperado.



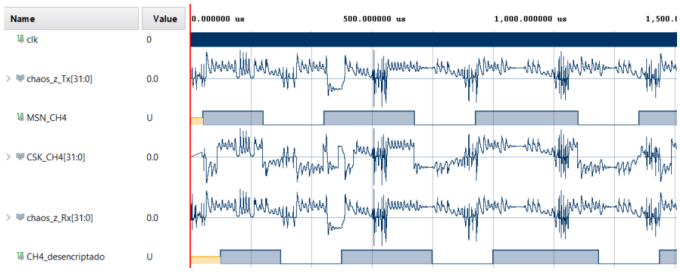
(a)



(b)



(c)



(d)

Figura 12: Simulación de modulación y demodulación CSK en VHDL (a) canal 1, (b) canal 2, (c) canal 3 y (d) canal 4.

La arquitectura resultante se muestra en la Figura 13 generada por el software de Vivado. Para los diseños se utiliza lenguaje VHDL y condiciones de punto fijo de 32 bits, 21 para la parte entera, 10 para la parte fraccionaria y 1 bit para el signo.

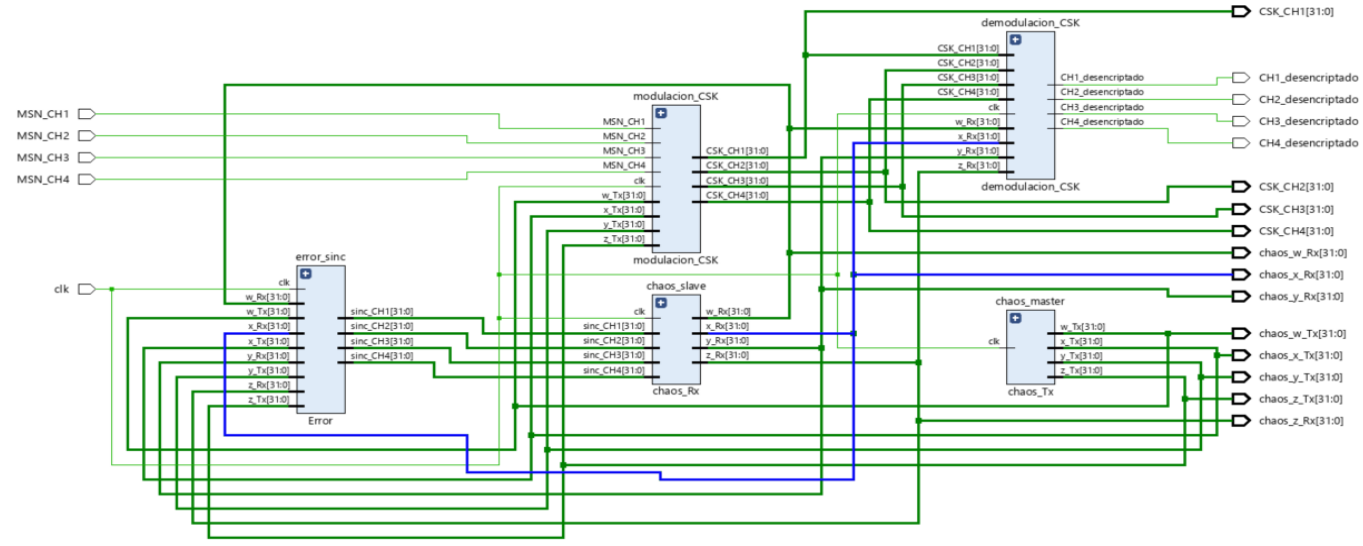


Figura 13: Arquitectura del circuito de modulación y demodulación CSK con portadora reconfigurable.

En la Tabla 3 se muestran los recursos lógicos utilizados por todo el sistema y por entidad requeridos por la tarjeta Artix-AC701 con chip xc7a200tfbg676.

Tabla 3: Recursos lógicos del sistema completo.

Entidad	LUT (134600)	Registros (269200)	DSP (740)	I/O (400)	BUFF (32)
MAIN	22190 (16%)	1638 (1%)	562 (76%)	65 (16.25%)	12 (38%)
Chaos_master	6426	503	280	0	0
Chaos_slave	6792	539	282	0	0
Error_sinc	145	96	0	0	0
Mod_CSK	176	164	0	0	0
Demod_CSK	450	336	0	0	0

9. Conclusiones

En esta investigación se consiguió una sincronización con portadoras caóticas reconfigurables, para este caso se intercambiaron los parámetros del oscilador principal para imitar 6 osciladores caóticos distintos, 3 en 3D y los otros 3 en 4D. La implementación de los 6 osciladores fue arbitraria, sin embargo, un aspecto de mayor importancia fue la metodología para implementar osciladores tanto en 3D como en 4D utilizando un mismo oscilador caótico. Adicionalmente se utilizaron estas portadoras reconfigurables en una técnica de modulación caótica CSK con previa encriptación mediante una operación X-OR y se consiguió recuperar un tren de pulsos en binario. La tarjeta FPGA utilizada fue una Artix-7 AC701 con chip xc7a200tfbg676 la cual cuenta con un reloj de 200 MHz y con ello se consiguió una velocidad de procesamiento de 20 kbit/s. Sin embargo, esta velocidad de procesamiento depende de la velocidad de reloj utilizada, en donde cada bit requiere de 10 mil ciclos de reloj. Los recursos lógicos requeridos para el sistema de modulación y demodulación no superan el máximo disponible en la tarjeta. Como trabajo futuro se mejorarán las características de la modulación, tales como la velocidad de transmisión al utilizar símbolos y conseguir transmitir mas de un bit por segmento de señal caótica. Por otro lado, si se utiliza un pulso de reloj externo de mayor velocidad que la tarjeta Artix-7 AC701 se podrán obtener mayores velocidades de procesamiento.

Agradecimientos

Los autores agradecen el Instituto Politécnico Nacional por el apoyo recibido mediante el proyecto SIP 20230135.

Referencias

Abedini, M., Gomroki, M., Salarieh, H., Meghdari, A., (2014). Identification of 4D Lü hyper-chaotic system using identical systems synchronization and fractional adaptation law. Applied Mathematical Modelling. Vol. 38, pp. 4652-4661.

Effati, S., Saberi, J., Saberi, H., (2014). Optimal and adaptive control for a kind of 3D chaotic and 4D hyper-chaotic systems. Applied Mathematical Modeling, no. 2, vol. 38, pp. 759-774.

Hu, H., Liu, N., Ding, N., (2013). Pseudorandom sequence generator based on the Chen chaotic system. Computer Physics Communications, no. 3, vol. 184, pp. 765-768.

Kaddoum, G., Tadayon, N., (2017). Differential Chaos Shift Keying: a robust modulation scheme for power-line communications. IEEE Transactions on circuits and systems, no. 1, vol. 64, pp. 31-35.

Lai, Q., Nestor, T., Kengne, J., Zhao, X. W., (2018). Coexisting attractors and circuit implementation of a new 4D chaotic system with two equilibria. Chaos, Solitons and Fractals, vol. 107, pp. 92-102.

Liu, J., *et al*., (2002). Bridge the gap between the Lorenz system and the Chen system. International Journal of Bifurcation and Chaos, no. 12, vol. 12, pp. 2917-2926.

Posadas, Castillo, C., *et al*., (2014). Synchronization of Irregular Complex Networks with Chaotic Oscillators: Hamiltonian Systems Approach. Journal of applied research and technology, no. 4, vol. 12, pp. 782-791.

Qi, G., Chen, G., (2015). A spherical chaotic system. Nonlinear Dynamics, no. 81, vol. 2015, pp 1381-1392.

Qi, G., Chen, G., (2006). Analysis and circuit implementation of a new 4D chaotic system. Physics letters A, no. 4, vol. 352, pp. 386-397.

Rezk, A. A., *et al*., (2019). Reconfigurable chaotic pseudo random number generator based on FPGA. International Journal of Electronics and Communications (AEÜ), vol. 98, pp. 174-180.

Wang, M., *et al*., (2019). Dynamics and circuit implementation of a four-wing memristive chaotic system with attractor rotation. International Journal of Non-Linear Mechanics, no. 111, vol. 2019, pp. 149-159.

Wang, Z., *et al*., (2010). A new type of four-wing chaotic attractors in 3-D quadratic autonomous systems. Nonlinear Dynamics, no. 60, vol. 2010, pp. 443-457.

Xu, L., Zhang, J., (2022). A Novel four Wing chaotic system with multiple attractors based on hyperbolic sine: Application to image encryption. Integration, vol. 87, pp. 313-331.

Xu, Y., Zhang, M., Li, C., (2016). Multiple attractors and robust synchronization of a chaotic system with no equilibrium. Optik, vol. 127, pp. 1363-1367.

Zhang, K., Wang, H., Fang, H., (2012). Feedback control and hybrid projective synchronization of a fractional-order Newton-Leipnik system. Common Nonlinear Sci Number Simulat, no. 1, vol. 17, pp. 317-328.

Zhang, S., *et al*., (2018). Generating one to four-wing hidden attractors in a novel 4D no-equilibrium chaotic system with extreme multistability. Chaos, no. 28, vol. 2018, pp. 1-11.

Zhou, L., Chen, Z., Wang, Z., Wang, J., (2016). On the analysis of local bifurcation and topological horseshoe of a new 4D hyper-chaotic system. Chaos, Solitons and Fractals, vol. 91, pp. 148-156.