Retos en el diseño de un generador caótico en tecnología CMOS submicrónica

Francisco Aznar
Centro Universitario de la Defensa
Grupo de Diseño Electrónico
Universidad de Zaragoza
Email: faznar@unizar.es

Carlos Sánchez-Azqueta, Cecilia Gimeno
Departamento de Ingeniería Electrónica y Comunicaciones
Grupo de Diseño Electrónico
Universidad de Zaragoza
Email: csanaz@unizar.es, cegimeno@unizar.es

***Resumen*—En este artículo se exponen los retos para llevar a cabo el diseño de un generador caótico, basado en el circuito de Chua, en tecnología CMOS submicrónica. El diseño analógico del generador caótico se complementa con un control digital, que proporciona programabilidad para definir distintos estados (claves) que aumenten la seguridad del cifrado. Además, se analizan distintas variables (temperatura, mismatching...) que pueden afectar a la sincronización de dos sistemas idealmente idénticos, impidiendo el descifrado de la información transmitida.**

***Palabras clave*—Circuito de Chua, comunicación segura, generador caótico, tecnología CMOS *(Chaotic generator, Chua's circuit, CMOS technology, secure communication)*.**

I. Nomenclatura

CMOS	Complementary Metal-Oxide Semiconductor
PSSR	Power Supply Rejection Ratio
VHF	Very High Frequency
FHSS	Frequency-Hopping Spread System

II. Introducción

Las comunicaciones representan un pilar esencial de nuestra sociedad. En particular, garantizar la privacidad se ha convertido en una temática de investigación prioritaria. Hasta el punto de que se trata de uno de los retos identificados en la Estrategia Española de Ciencia y Tecnología y de Innovación. De igual manera se consideran las TICs aplicables a este reto como una de las Tecnologías Facilitadoras Esenciales identificadas en el Programa Europeo Horizonte 2020. Esto se debe a que la seguridad de las comunicaciones es fundamental en algunas aplicaciones en el ámbito civil (transmisión de datos bancarios, datos personales...) y toma mayor relevancia en el ámbito militar. Existen multitud de sistemas de cifrado adaptados al nivel de seguridad necesario para cada aplicación concreta. Los avances en los algoritmos y potencia de cálculo de los descifradores exigen una continua mejora de los métodos de cifrado.

En el ámbito de la defensa, las comunicaciones por radio se transmiten cifradas en un rango de frecuencia reservado de la banda VHF (30 - 88 MHz). El método de cifrado es doble, por un lado se usa el FHSS, que consiste en transmitir la información sobre una onda portadora cuya frecuencia va cambiando aleatoriamente siguiendo un patrón conocido por el emisor y el receptor. Este método evita que la señal se intercepte, por lo que impide, no solo que se conozca la información transmitida, sino también la capacidad de localizar el emisor mediante triangulación. Además, la señal transmitida se envía cifrada mediante un método solo conocido por el fabricante del sistema de radio.

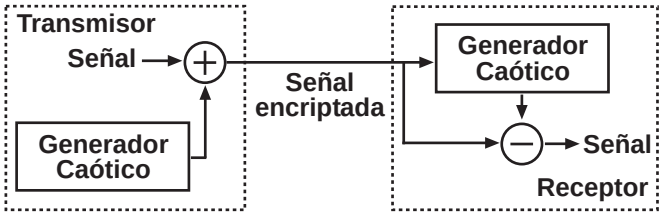

Figura 1. Esquema conceptual de una transmisión basada en cifrado caótico

Las señales caóticas, dada su naturaleza impredecible y su amplio ancho de banda, son candidatas idóneas para cifrar señales vulnerables [1]. El sistema de comunicaciones (figura 1) se basa en dos generadores caóticos idénticos y sincronizados [2]. La señal a transmitir se mezcla con la señal caótica (representado simbólicamente como una suma) y se recupera la señal transmitida mediante el desacoplo de la misma señal caótica (representado simbólicamente como una resta). Ya se ha demostrado que el cifrado caótico no es 100 % seguro [3], [4], pero incluir este sistema puede ofrecer un aumento del nivel de seguridad por complementariedad a los métodos ya implementados.

El proceso de fabricación de circuitos integrados dominante en la actualidad es el CMOS. Se basa en la construcción de los elementos activos basados en transistores MOS en una misma oblea de material semiconductor (silicio) mediante difusiones donadoras (N) y aceptoras (P), un aislante (oxido de silicio) y un material conductor (polisilicio). Además, se añaden varias capas de metalización para la interconexión de los distintos elementos (figura 2). Esta tecnología ofrece las prestaciones necesarias para trabajar en un rango de alta frecuencia con bajo consumo [5].

En este artículo se presenta el inicio de una línea de investigación que tiene por objeto desarrollar un sistema de comunicaciones seguro basado en tecnología CMOS. En la

ISBN: 978-84-9717-323-0

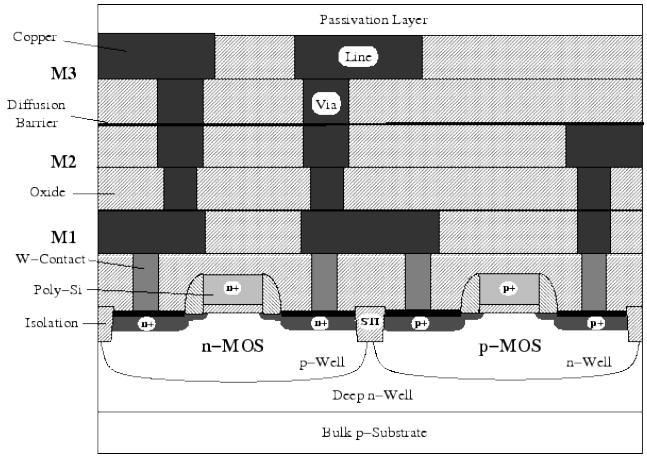

Figura 2. Sección de un proceso de fabricación CMOS con tres niveles de metalización

sección III se aborda el diseño del generador caótico en tecnología CMOS submicrónica, incorporando programabilidad para dotar al sistema de multiples claves criptográficas. En la sección IV se analizan los aspectos más relevantes que afectan al comportamiento de dos generadores caóticos teóricamente idénticos, por lo que se perdería el sincronismo, y por lo tanto no se podría recuperar la señal transmitida. Por último, las conclusiones son expuestas en la sección V.

III. Diseño del generador caótico

El generador caótico en el que nos basamos es el circuito de Chua, mostrado en la figura 3, que representa el circuito electrónico caótico más sencillo ya que cumple los requisitos mínimos necesarios: un sistema de tres ecuaciones diferenciales de primer orden, formado por L, C_1 y C_2, y un elemento no lineal (R_N). Las ecuaciones que describen la dinámica del sistema son:

$$\begin{aligned} C_1\frac{dv_1}{dt} &= \frac{1}{R}(v_1 - v_2) - f(v_1) \\ C_2\frac{dv_2}{dt} &= \frac{1}{R}(v_1 - v_2) + i_3 \\ L\frac{di_3}{dt} &= -v_2 \end{aligned} \quad (1)$$

Siendo f la función que define la resistencia no lineal. La solución de este sistema de ecuaciones diferenciales puede presentar un comportamiento caótico, tal y como se demuestra en [6].

III-A. Implementación microelectrónica del circuito de Chua

La industria microelectrónica ha realizado un increíble avance tecnológico en los últimos años. Sin embargo, dicho avance se centra básicamente en la miniaturización del transistor MOS, dotando de mejores prestaciones a los circuitos digitales fundamentalmente. Si queremos diseñar en tecnología CMOS un circuito analógico como el circuito de Chua, nos encontramos con serias limitaciones a la hora de implementar elementos tan comunes como resistencias y condensadores.

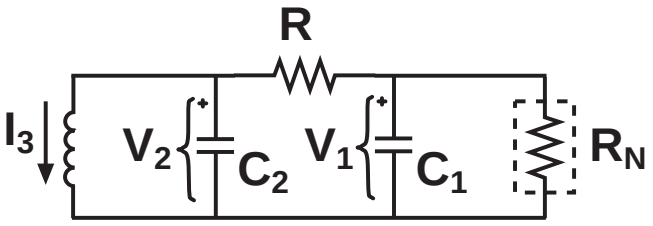

Figura 3. Circuito de Chua

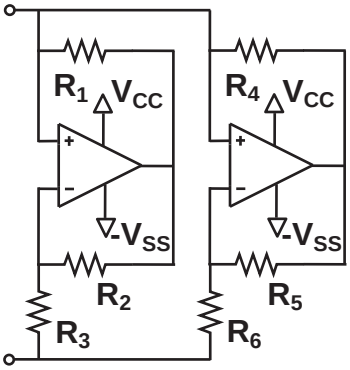

Figura 4. Implementación de la resistencia no lineal mediante amplificadores operacionales

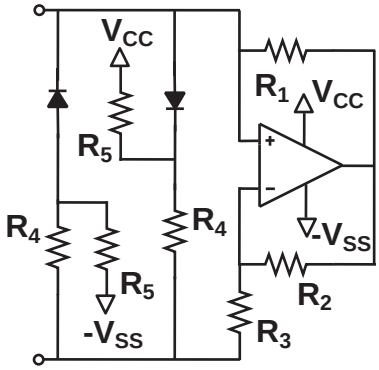

Figura 5. Implementación de la resistencia no lineal incluyendo diodos

Afortunadamente, el hecho de que para cubrir algunas aplicaciones sea imprescindible contar con electrónica analógica ha propiciado que el proceso de fabricación CMOS ofrezca la implementación de resistencias fabricadas en polisilicio, condensadores plano-paralelos entre dos de sus niveles de metalización (o bien, dos capas de polisilicio) e inductores basados en pistas metálicas con forma espiral.

El orden de magnitud de la resistencia por cuadro ($1k\Omega$) y la capacidad por unidad de área ($1fF/\mu m^2$) que ofrece un proceso CMOS de coste moderado conlleva que el área ocupada por el circuito sea considerable. Por lo tanto, para minimizar el coste final, que está directamente relacionado con

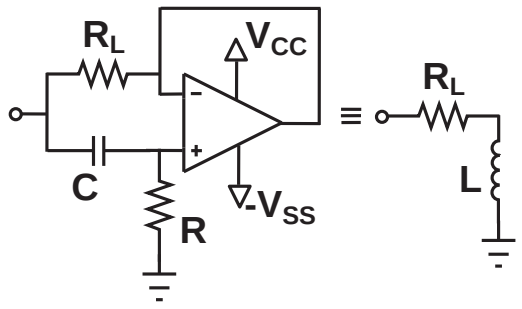

Figura 6. Implementación del inductor mediante amplificadores operacionales

el área ocupada, deberemos buscar estrategias de optimización. Pero el gran reto de la implementación microelectrónica del circuito de Chua viene de la mano de la resistencia no lineal y, especialmente, el inductor. La implementación de una resistencia no lineal se puede llevar a cabo mediante dos resistencias negativas en paralelo [7], basándonos en amplificadores operacionales (figura 4). Otra posibilidad es utilizar diodos [8] (figura 5), los cuales aportan la característica no lineal, derivado de su comportamiento asimétrico en cuanto a la conducción de la corriente. En la literatura se pueden encontrar diversos trabajos que demuestran el comportamiento caótico con elementos discretos, por ejemplo para transmisión de audio en frecuencia modulada [9]. La resistencia no lineal también se puede implementar con amplificadores de transconductancia [10], formados únicamente por transistores, lo que facilita la integración en tecnología CMOS [11], [12].

El inductor es difícil de implementar debido a su naturaleza de elemento tridimensional. Existen implementaciones en tecnología CMOS basadas en estructuras bidimensionales, pero ofrecen pobres prestaciones y contribuyen a aumentar el área del circuito significativamente (para inductancias de nH, factor de calidad limitado en torno a 10 y radios 100 μm aproximadamente). Basándonos también en amplificadores operacionales podemos emular un inductor [13] a partir de resistencias y condensadores (figura 6). El valor de la inductancia viene determinado por la expresión $L = CRR_L$. Esta alternativa optimiza el área integrada manteniendo una filosofía de integración común.

III-B. Programabilidad

Dado que los valores de los elementos que componen el sistema caótico son la clave para descifrar la transmisión, una manera de aumentar la seguridad de la comunicación es dotar al sistema de múltiples estados, ofreciendo la posibilidad de cifrar la transmisión bajo más de una clave criptográfica. O, lo que es lo mismo, implementar un circuito programable.

La programabilidad más robusta está basada en una señal digital de control formada por un número determinado de bits, los cuales ofrecen dos estados claramente definidos. Para una señal digital de n bits, dependiendo del código usado, podemos tener hasta 2^n posibles claves. Por tanto, la implementación del circuito de Chua programable tiene carácter mixto (analógico-digital).

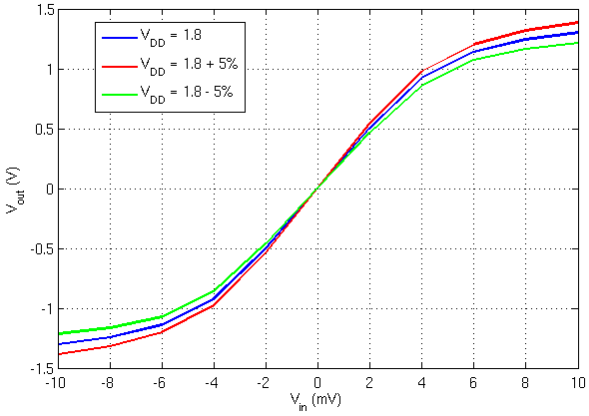

Figura 7. Variación de la relación entrada-salida para un amplificador diferencial CMOS bajo una fluctuación del $\pm 5\,\%$ en el voltaje de alimentación

La programabilidad digital está basada en el hecho de que los transistores actúan como conmutadores entre dos estados (conducción y corte) en función del estado de la señal de control asociada. Así, resultando en que uno (o varios) elementos del circuito de Chua varían su valor al formarse por varios elementos que están interconectados en paralelo cuando los transistores asociados están en conducción. En la literatura se encuentran trabajos realizados en tecnología CMOS que incluyen programabilidad digital y trabajan en rangos frecuenciales elevados [14], [15].

IV. Sincronismo

L. M. Pecora y T. L. Carroll demostraron en 1990 que dos circuitos caóticos idénticos se sincronizan [16], es decir, ofrecen un comportamiento dinámico idéntico. La señal transmitida cifrada puede actuar directamente como elemento sincronizador, como ya se reflejaba en la figura 1. El sincronismo se degrada cuando los circuitos caóticos difieren. Por lo tanto, queremos implementar un circuito programable con diferentes estados que sólo sincronicen con los estados equivalentes. Para ello debemos estudiar y analizar el impacto que tienen diferentes factores que afectan a los valores de los elementos que forman el circuito caótico. Los factores más relevantes son el voltaje de alimentación, la temperatura y la tolerancia propia de la fabricación microelectrónica.

IV-A. Voltaje de Alimentación

Los elementos activos requieren un voltaje de alimentación para su funcionamiento. La variación del valor de esa tensión puede afectar a su punto de operación, y por tanto, al comportamiento del sistema caótico. El parámetro que cuantifica la inmunidad del circuito activo frente a variaciones del voltaje de alimentación (V_{DD}) es el $PSRR$, definido como:

$$PSRR(dB) = 20log_{10}(A_V \frac{\Delta V_{DD}}{\Delta V_O}) \qquad (2)$$

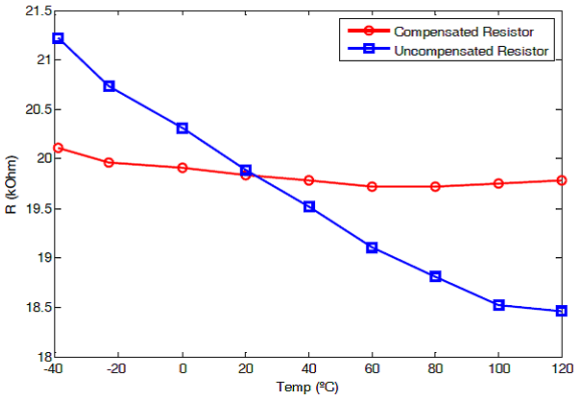

Figura 8. Variación con la temperatura para una resistencia propia de la tecnología (no compensada) y una combinación de dos resistencias con dependencia complementaria (compensada)

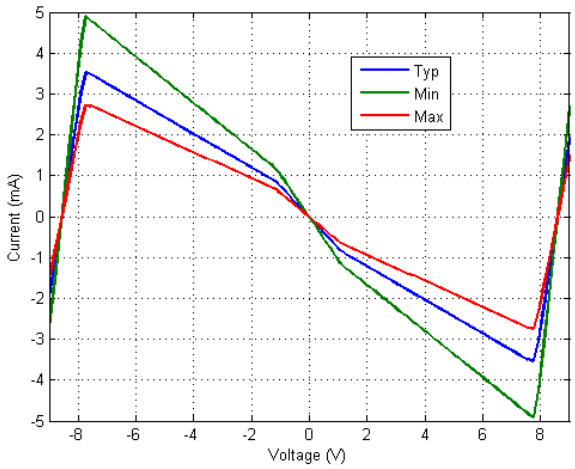

Figura 9. Curva intensidad-tensión para la resistencia no lineal para los valores nominales y corners

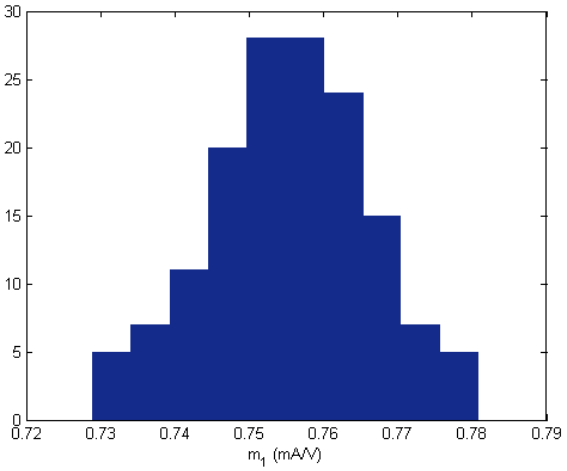

Figura 10. Distribución del valor de la pendiente para pequeña señal de la resistencia no lineal según la simulación de Montecarlo

Siendo V_O y A_V el voltaje de salida y la ganancia del circuito activo, respectivamente.

El bloque constituyente básico de un amplificador operacional es un amplificador diferencial. La figura 7 muestra la variación de la respuesta de un amplificador CMOS diferencial para una fluctuación del voltaje de alimentación de $\pm 5\,\%$. Esto lleva a un resultado en torno a $PSRR = 51dB$. Los amplificadores operacionales comerciales basados en transistores CMOS [17] ofrecen un PSRR de 75 dB como valor típico, lo que garantiza esta tecnología puede ofrecer una inmunidad sufienciente frente a variaciones del voltaje de alimentación.

IV-B. Temperatura

La temperatura de trabajo puede variar considerablemente dependiendo del entorno. Como ejemplo, el rango de temperaturas de trabajo para una circuito digital de aplicación civil cubre de 0 a 70 ºC, mientras que para aplicaciones militares se extiende de -55 a 125 ºC.

Los elementos que se ven alterados por los cambios de temperatura son las resistencias, los amplificadores de tranconductancia [18] y los diodos que forman parte de la resistencia no lineal. El valor de los condensadores se rige por factores geométricos y por el valor de la constante dieléctrica, mientras que los amplificadores operacionales se diseñan con una ganancia muy elevada, lo que ofrece inmunidad ante dicho valor por lo que el comportamiento del circuito activo viene determinado por los elementos pasivos que lo acompañan (resistencias y condensadores).

Las resistencias implementadas en tecnología microelectrónica ofrecen una dependencia con la temperatura caracterizada por el propio fabricante. Afortunadamente, existen varios tipos de resistencias que ofrecen un comportamiento con la temperatura complementario. Así, combinando ambos tipos podemos implementar resistencias con un valor muy constante en el rango de temperaturas de trabajo [19], tal y como queda reflejado en la figura 8.

Una implementación del circuito de Chua basada en amplificadores de transconductancia ofrecerá una variabilidad frente a cambios de temperatura. Los diodos ven modificada su respuesta ya que la temperatura afecta a la tensión umbral y a la corriente inversa de saturación. Este efecto podríamos considerarlo despreciable para el comportamiento del generador caótico, pero la construcción de la resistencia no lineal sin diodos ofrece un comportamiento más robusto en función de la temperatura, siendo por tanto la opción predilecta.

IV-C. Mismatching

La repetitibilidad de los valores a la hora de fabricar elementos electrónicos no esta garantizada. De hecho, las tolerancias de fabricación de elementos discretos varían entre un $10\,\%$ y un $1\,\%$. La industria microelectrónica propicia una minimización de la variabilidad de los parámetros, derivada de la fabricación simultánea de varios circuitos. Además se siguen criterios de optimización tales como respetar la orientación, no usar dimensiones mínimas y estructuras en centroide común.

Así, las tolerancias se minimizan, sobre todo para los valores relativos entre elementos fabricados en una misma oblea. Los fabricantes ofrecen modelos para el simulado de la variabilidad de los parámetros bajo criterios extremos (corner) y con dispersión gaussiana siguiendo modelos de Montecarlo.

Como ejemplo, la figura 9 muestra el efecto de las variaciones corner sobre la resistencia no lineal, fundamentalmente causadas por la variación del valor de las resistencias. Esta simulación conlleva una variación de la pendiente para pequeña señal (denominada m_1) de $-22\,\%$ y $37{,}5\,\%$ respecto del valor nominal. Estos valores están sobreestimados ya que representan casos extremos. Una simulación de Montecarlo ofrece una dispersión gaussiana (figura 10) de menos de $3\,\%$ (bajo el criterio de dos veces la desviación típica) sin implementar técnicas de minimización. Al implementar dichas técnicas, quedaría garantizada una baja dispersión de los parámetros de la resistencia no lineal.

V. Conclusiones

El factor determinante para la viabilidad de un sistema basado en cifrado caótico es el sincronismo entre transmisor y receptor. La arquitectura del generador caótico basada en resistencias, condensadores y amplificadores operacionales se postula como la más robusta. Un PSRR elevado, la compensación de la dependencia con la temperatura de la resistencia y la minimización de la dispersión causada por la fabricación del circuito integrado son los factores detectados como clave durante la etapa de diseño en un proceso CMOS submicrónico. Una tecnología CMOS actual de bajo coste ofrece altas prestanciones en términos de frecuencia y consumo. Además, se incluye la posibilidad de incluir programabilidad para aumentar la seguridad de la transmisión.

Agradecimientos

Los autores agradecen la ayuda concedida por el Centro Universitario de la Defensa (2013-12) para iniciar esta línea de investigación, asi como la colaboración del Grupo de Diseño Electrónico mediante el proyecto del Plan Nacional de I+D+i TEC2011-23211. Además, agradecer la colaboración del Capitán Javier Gil Marín, especialista en transmisiones de la Academia General Militar, por el asesoramiento ofrecido.

Referencias

[1] T. Yang, "A Survey of Chaotic Secure Communication Systems," *International Journal of Computational Cognition*, vol. 2, no. 2, pp. 81–130, 2004.

[2] A. Riaz, M. Ali, "Chaotic Communications, their Applications and Advantages over Traditional Methods of Communication," en *Proceedings of 6th International Symposium on Communications Systems, Networks and Digital Signal Processing (CNSDSP2008)*, 2008, pp. 21–24.

[3] G. Álvarez, F. Montoya, G. Pastor, M. Romera, "Breaking a secure communication scheme based on the phase synchronization of chaotic systems," *Chaos*, vol. 14, no. 2, pp. 274–278, 2004.

[4] A. B. Orúe, M.J. García-Martínez, G. Pastor, F. Montoya, C. Sánchez Ávila, "Criptoanálisis de un criptosistema de dos canales basado en una función no lineal caótica," en *Actas de la XII Reunión Española sobre Criptología y Seguridad de la Información (RECSI2012)*, U. Zurutuza, R. Uribeetxeberria, I. Arenaza-Nuño, Eds. Arrasate - Mondragon: Servicio Editorial de Mondragon Unibertsitatea, 2012, pp. 119–124.

[5] F. Aznar, S. Celma, B. Calvo, "CMOS Receiver Front-ends for Gigabit Short-Range Optical Communications," New York, NY: Analog Circuits and Signal Processing Series, Springer, 2013.

[6] L. O. Chua, G. Lin, "Canonical Realization of Chua's Circuit Family," *IEEE Transaction of Circuits and Systems*, vol. 37, no. 7, pp. 885–902, 1990.

[7] M. P. Kennedy, "Robust OpAmp Realization of Chua's Circuit," *Frequenz*, vol. 46, no. 3-4, pp. 66–80, 1992.

[8] P. Bratissol, L. O. Chua, "The double hook [nonlinear chaotic circuits]," *IEEE Transactions on Circuits and Systems*, vol. 35, no. 12, pp. 1512–1522, 1988.

[9] P. Khumsat, G. Nowlkeaw, "Chaotic radio for audio communications," en *IEEE Region 10 Conference (TENCON2007)*, 2007, pp. 1–4.

[10] J. M. Cruz, L. O. Chua, "A CMOS IC Nonlinear Resistor for Chua's Circuit," *IEEE Transactions on Circuits and Systems - I: Fundamental Theory and Applications*, vol. 39, no. 12, pp. 985–995, 1992.

[11] A. Rodríguez-Vázquez, M. Delgado-Restituto, "CMOS Design of Chaotic Oscillators Using State Variables: A Monolithic Chua's Circuit," *IEEE Transactions on Circuits and Systems - II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 596–613, 1993.

[12] J. M. Cruz, L. O. Chua, "An IC Chip of Chua's Circuit," *IEEE Transactions on Circuits and Systems - II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 614–625, 1993.

[13] B. Muthuswamy, T. Blain, K. Sundqvist, "A Synthetic Inductor Implementation of Chua's Circuit," Technical Report No. UCB/EECS-2009-20, Electrical Engineering and Computer Sciences, University of California at Berkeley, 2009. Disponible en http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-20.html.

[14] B. Calvo, S. Celma, F. Aznar, J.P. Alegre, "Low-voltage CMOS programmable gain amplifier for UHF applications," *Electronics Letters*, vol. 43, no. 20, pp. 1087–1088, 2007.

[15] A. Otin, S. Celma, C. Aldea, "CMOS filter with wide digitally programmable VHF range," *Electronics Letters*, vol. 43, no. 1, pp. 21–23, 2007.

[16] L. M. Pecora, T. L. Carroll, "Synchronization in Chaotic Systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, 1990.

[17] Texas Instruments, "250MHz, Rail-to-Rail I/O, CMOS Opertional Amplifiers," Datasheet, 2009. Disponible en http://www.ti.com/lit/ds/symlink/opa354.pdf.

[18] Texas Instruments, "LM13700 Dual Operational Transconductance Amplifiers with Linearizing Diodes and Buffers," Datasheet, 2013. Disponible en http://www.ti.com/lit/ds/symlink/lm13700.pdf.

[19] C. Azcona, B. Calvo, S. Celma, "Voltage-to-Frequency Converters," New York, NY: Analog Circuits and Signal Processing Series, Springer, 2013.