(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 644 485**

(51) Int. CI.:

G06F 7/58 (2006.01)
H03K 3/84 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.05.2007 PCT/IB2007/051938**

(87) Fecha y número de publicación internacional: **27.11.2008 WO08142488**

(96) Fecha de presentación y número de la solicitud europea: **22.05.2007 E 07735990 (9)**

(97) Fecha y número de publicación de la concesión europea: **19.07.2017 EP 2176739**

(54) Título: **Procedimiento y equipo para generar números aleatorios utilizando la arquitectura de un doble oscilador y caos de tiempo continuo**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.11.2017

(73) Titular/es:

TUBITAK (100.0%)
Ataturk Bulvari No. 221, Kavaklidere
06100 Ankara, TR

(72) Inventor/es:

ERGUN, SALIH

(74) Agente/Representante:

MARTÍN SANTOS, Victoria Sofia

DESCRIPCIÓN

Procedimiento y equipo para generar números aleatorios utilizando la arquitectura de un doble oscilador y caos de tiempo continuo

En la última década, la creciente demanda de transacciones electrónicas oficiales y financieras, el uso de aplicaciones de firma digital y las necesidades del secreto de la información han hecho muy populares a los generadores de números aleatorios (RNG por sus siglas en inglés de *Random Number Generators*). Con este respecto, los RNG, que han sido utilizados generalmente para aplicaciones criptográficas militares en el pasado, tienen ahora un papel importante en el diseño de un equipo habitual de comunicación digital.

Casi todos los sistemas criptográficos requieren valores impredecibles, por lo tanto, RGN es un componente fundamental de los mecanismos criptográficos. La generación de claves / pares de operadores públicos y privados para los algoritmos asimétricos y claves para los sistemas de cifrado simétricos e híbridos requieren números aleatorios. Los generadores de contraseñas las impugnaciones, los valores aleatorios utilizados sólo una vez, los bytes [octetos] de relleno y los valores en blanco se crean mediante el uso de generadores de números realmente aleatorios (TRNG por sus siglas en inglés de *Truly Random Number Generators*) [1]. Los generadores de números pseudo-aleatorios (PRNG por sus siglas en inglés de *Pseudo-Random Number Generators*) generan los bits de una manera determinista. A fin de aparecer como generado por un TRNG, las secuencias pseudo-aleatorias deben ser diseminadas a partir de una secuencia verdaderamente aleatoria más corta [2]. Los RNG también se utilizan en muchas áreas, incluyendo el análisis Monte Carlo, simulaciones por ordenador, el muestreo estadístico, procedimientos de optimización estocástica, marcas de agua para la autenticación de imagen, procedimiento de autenticación entre dos equipos de cifrado y el valor de la aleatorización inicial de un módulo criptográfico que realiza un algoritmo.

Incluso si se conoce el diseño RNG, no se puede hacer una predicción útil sobre la salida. Para cumplir con los requisitos de secreto del generador de contraseñas, para la generación de claves y otras aplicaciones criptográficas, los TRNG deberán cumplir las siguientes propiedades: El flujo de bits de salida del TRNG debe pasar todas las pruebas estadísticas de aleatoriedad; el siguiente bit aleatorio debe ser imprevisible [3]; el mismo flujo de bits de salida del TRNG no debe ser capaz de reproducirse [4]. La mejor manera de generar números aleatorios verdaderos es explotar la aleatoriedad natural del mundo real mediante la búsqueda de un evento aleatorio que sucede regularmente [4]. Ejemplos de tal evento utilizables incluyen el tiempo transcurrido durante la desintegración radiactiva, ruido térmico y de tiro, la fluctuación de fase del oscilador y la cantidad de carga de un condensador semiconductor [2].

Existen pocos diseños de RNG mencionados en la literatura; sin embargo, fundamentalmente se mencionaron cuatro técnicas diferentes para generar números aleatorios: amplificación de una fuente de ruido [5, 6] arquitectura de doble oscilador [1, 7, 8, 9], mapas caóticos de tiempo discreto [10, 11, 12, 13, 14] y los osciladores caóticos de tiempo continuo [15, 18]. A pesar del hecho de que el uso de mapas caóticos de tiempo discreto en la realización de RNG es bien conocido desde hace algún tiempo, recientemente se demostró que los osciladores caóticos de tiempo continuo también pueden usarse para realizar TRNG. Siguiendo en esta dirección, investigamos la utilidad de la innovación propuesta para generar datos binarios aleatorios de osciladores caóticos de tiempo continuo con arquitectura de doble oscilador.

Las velocidades de bits de generadores de números aleatorios que se encuentran comúnmente en la literatura y en productos comerciales se convirtieron en insuficientes debido a las crecientes tasas de datos en equipos digitales de comunicación. En comparación con los generadores de números aleatorios basados en mapas caóticos de tiempo discreto, la amplificación de una fuente de ruido y el muestreo del oscilador jitter, se ve que los RNG basados en osciladores caóticos de tiempo continuo pueden ofrecer tipos de datos constantes mucho más altos y sin post-procesamiento con circuitos integrados menos complejos. En conclusión, se puede deducir que los osciladores caóticos de tiempo continuo pueden ser integrados en los procesos de hoy en el rango GHz y el uso de caos de tiempo continuo con las innovaciones propuestas es muy prometedor en la generación de números aleatorios con un rendimiento muy alto.

Para ser compatible con otros elementos del sistema, es preferible usar osciladores caóticos que se puedan integrar en silicio. Se han realizado varios intentos para introducir discretos tiempos, así como osciladores caóticos CMOS de tiempo continuo. En la mayoría de estos intentos, los circuitos resultantes fueron complicados y ocuparon una gran área de silicio. Los osciladores caóticos de tiempo discreto generalmente emplean técnicas de corriente alterna o de conmutación. La utilización de un multiplicador, además de los muchos condensadores y op amps *(amplificadores operacionales)*, da como resultado automáticamente un circuito grande. En comparación con los RNG basados en fuentes caóticas de tiempo discreto, se observa que los RNG basados en fuentes caóticas de tiempo continuo pueden ofrecer velocidades de datos mucho más altas con circuitos integrados menos complejos y menos ruidosos, en particular debido a la ausencia de muestreo y retención sucesivos etapas

La amplificación de una técnica de fuente de ruido se muestra en la figura 1, utiliza un amplificador de alto ancho de banda de alta ganancia para procesar el ruido blanco que tiene tensión de corriente alterna pequeña. El ruido debe ser amplificado a un nivel donde puede ser un umbral de precisión sin desviación por un comparador de reloj. Esta es la técnica RGN más popular para las soluciones de un solo chip o a nivel de placa.

En circuitos integrados CMOS de baja tensión, dos mecanismos diferentes de ruido de banda ancha generan ruido blanco: ruido de disparo (generado por el flujo de corriente a través de una unión p-n) y ruido térmico (generado por el movimiento de electrones en una resistencia aleatoria). Ruido de avalancha no es una opción práctica para una fuente de ruido debido a la tensión típica de alta descomposición (> 6V DC) de diodos Zener fabricados en procesos CMOS a granel. Como se muestra en la figura 1, la topología de la fuente de ruido integrado utiliza una gran resistencia como un generador de ruido térmico. Las resistencias se fabrican fácilmente a partir de capas de polisilicio o de difusión y no requieren corriente de polarización para generar ruido, como lo hacen las uniones semiconductoras. Una resistencia de polisilicio también tiene un índice de ruido de parpadeo bajo (típicamente -30 dB), asegurando niveles bajos de ruido 1/f.

Suponiendo un escaso ruido 1/f, la tensión de ruido térmico de la resistencia de fuente R_{Src} sería $E_t = \sqrt{4kTR_{Src}\Delta f}$ dónde k es la constante de Boltzmann, T es la temperatura absoluta, R_{Src} es la resistencia, y Δf es el ancho de banda de ruido. El ancho de banda de ruido de E_t está limitado normalmente por el primer filtro de orden de paso bajo formado por R_{Src} y la capacidad de entrada del amplificador equivalente C_{Amp}. Siempre que el ancho de banda de -3dB del amplificador sea mayor que el ancho de banda de ruido, la tensión total de ruido equivalente E_{ni} debido a E_t en la entrada del amplificador será $E_{ni} = \sqrt{\frac{kT}{C_{Amp}}}$ donde es el límite teórico para el ruido térmico generado por una resistencia derivada de un condensador. La amplitud de voltaje de ruido térmico en un ancho de banda de 1 Hz se puede aumentar al aumentar el valor de R_{Src}, pero a costa del ancho de banda de ruido térmico reducido, de forma que E_{ni} se mantendrá constante para un determinado C_{Amp}.

La arquitectura del doble oscilador usa una fuente aleatoria que se deriva de dos osciladores de funcionamiento libre, uno rápido y el otro más lento, como se muestra en la figura 2. Los diseños de RNG publicados que usan esta técnica indican que los niveles típicos de fluctuación del oscilador no son casi suficientes para producir aleatoriedad estadística. Por esta razón, se utiliza una fuente de ruido para modular la frecuencia del reloj más lento, y con el borde ascendente del reloj más lento modulado por ruido, se muestrea el reloj rápido. La deriva entre los dos relojes proporciona así la fuente de dígitos binarios aleatorios. De manera similar a la amplificación de una técnica de fuente de ruido, el ruido debe amplificarse hasta un nivel donde pueda usarse para modular la frecuencia del reloj más lento. La frecuencia de reloj más lento, que determina la velocidad de transmisión de datos, está básicamente limitada por el ancho de banda de la señal de ruido utilizada para la modulación, donde la razón principal de la limitación es el ancho de banda del amplificador.

En la innovación propuesta de forma de onda del oscilador caótico, que es del orden de unos pocos voltios con una frecuencia central nominal en el rango de GHz, se explotó para modular la frecuencia del reloj más lento directamente sin usar un amplificador, donde el límite teórico para la velocidad de transmisión de datos está básicamente determinado por la frecuencia central nominal del oscilador caótico que resulta en el orden de 100 Gbit/s. Tales altas tasas de datos pueden hacer que los RNG de tiempo continuo sean atractivos en comparación con sus contrapartes basados en las otras técnicas. Tanto un oscilador caótico autónomo como uno no autónomo se pueden usar como núcleo del diseño del RNG propuesto.

Al comparar la innovación propuesta con el diseño de RNG anterior basado en un oscilador caótico de tiempo continuo dado en [15], la innovación propuesta ha sido verificada numéricamente para ser capaz de alcanzar velocidades 700 veces más altas. Además, la secuencia de bits de la muestra que aparece en http: //www.esat.kuleuven. ac.be/~mey/Ds2RbG/Ds2RbG.html falla en las pruebas de frecuencia de bloque, de funcionamiento y *ApEn* (por sus siglas in inglés de *Approximate Entropy* o Entropía Aproximada) del conjunto completo de pruebas NIST. Además, el ciclo de compensación no es factible para el diseño anterior dado en [15] debido a la razón de que la secuencia de bits obtenida puede sobrepasar el conjunto de pruebas completo de *Diehard* gracias al procesamiento de Von Neumann.

Mediante el uso de un oscilador caótico con la arquitectura de doble oscilador, el rendimiento de salida y la calidad estadística de las secuencias de bits generadas aumentan y el diseño propuesto es robusto contra interferencias externas, variaciones de parámetros y ataques dirigidos a forzar el rendimiento. En esta innovación, la señal de salida del oscilador caótico se utiliza para modular la frecuencia de un reloj más lento. Luego, con el borde ascendente del reloj más lento modulado por el caos, se muestrea el reloj rápido. Hemos desarrollado un modelo numérico para el diseño propuesto y finalmente hemos verificado de forma numérica y experimental que los datos binarios obtenidos por esta técnica de muestreo de oscilador, pasaron las pruebas utilizadas tanto en el conjunto de pruebas FIPS-140-2 [16] como en el conjunto completo de pruebas NIST de número aleatorio [17] para una mayor velocidad de rendimiento en comparación con los diseños de RNG anteriores basados en las otras técnicas.

Debido a su extrema sensibilidad a las condiciones iniciales y al tener un exponente positivo de Lyapunov y un espectro de potencia similar al ruido, los sistemas caóticos se prestan a ser explotados para la generación de

números aleatorios. Para obtener datos binarios aleatorios de un sistema caótico de tiempo continuo, hemos presentado una técnica interesante, que se basa en generar datos binarios no invertibles a partir de la forma de onda del oscilador caótico dado. Cabe señalar que la no invertibilidad es una característica clave para generar PRNG [19].

En la innovación propuesta, para obtener bits aleatorios binarios de un oscilador caótico autónomo o no autónomo, usamos la arquitectura de doble oscilador. En este diseño, la salida de un oscilador rápido se muestrea en el borde ascendente del reloj más lento modulado por el caos usando un *flip-flop* D o un *flip-flop* T. En un ejemplo, se usa un oscilador controlado por voltaje (VCO, pos sus siglas del inglés *voltage-controlled oscillator*) o un oscilador controlado por corriente (CCO por sus siglas del inglés *current-controlled oscillator*) para implementar la modulación de la frecuencia de reloj más lenta con la señal caótica que corresponde a uno del estado x_1, x_2, ... o, x_n, que son las cantidades normalizadas del oscilador caótico utilizado como núcleo del RNG propuesto. Hay que tener en cuenta que, aunque las trayectorias n-dimensionales en el plano x_1 - x_2 - ... - x_n son invertibles, se puede obtener una sección no invertible considerando solamente los valores correspondientes a uno de los estados, digamos x_1.

La frecuencia central del VCO (o CCO) determina la frecuencia central del reloj más lento. La deriva entre los dos osciladores proporciona generación de bits aleatorios para ser más robustos. Debido al fenómeno de alias no lineal asociado con el muestreo, la arquitectura del doble oscilador logra un mayor rendimiento y una mayor calidad estadística. En los diseños anteriores, una fuente de ruido se convierte en una secuencia binaria mediante el uso de un umbral, que básicamente es una conversión analógica a digital en dos bit quanta. Sin embargo, la arquitectura de doble oscilador proporciona la mayor parte de los componentes de frecuencia de la señal de entrada para afectar la salida.

Además, se ha desarrollado un modelo numérico para el diseño propuesto que permite la estimación de la entropía de bits de salida como una función de los parámetros de diseño. Suponiendo que VCO (o CCO) tiene una función de transferencia lineal, la frecuencia del reloj más lento f_{slow} se puede calcular de acuerdo con la siguiente ecuación 1:

$$f_{slow} = f_{slow\ center}\left(\frac{x_1}{2x_{1\ max}} + 1\right) \qquad (1)$$

en dónde $\frac{f_{slow}}{2} < f_{slow} < \frac{3f_{slow}}{2}$, para $-x_{1\ máx} < x_1 < x_{1\ máx}$. Entre los intervalos dados, el reloj más lento produce un valor de frecuencia de salida para cada valor x1. Si se conocen las frecuencias de reloj más rápidas y más lentas, así como la diferencia de fase de inicio ΔT, la salida del oscilador rápido, muestreada en el borde ascendente del reloj más lento modulado por el caos, se puede predecir como se ilustra en la figura 3. Se puede mostrar que los datos binarios $S_{(doble\ oscilador)i}$ son los inversos del bit menos significativo de la relación entre los períodos totales del reloj más lento y el período del reloj rápido:

$$S_{(dual\ oscillator)i} = \left(\left\lfloor \frac{\left(\sum_{j=1}^{i} T_{slow\ j}\right) - \Delta T}{T_{fast}/2} \right\rfloor mod2\right)' \qquad (2)$$

$$T_{slow\ j} = \frac{x_{1\ max}}{\frac{f_{slow\ center}}{2}(x_{1j} + 2x_{1\ max})}$$

donde el reloj rápido tiene un ciclo de trabajo del 50% y los valores x_{1j} se obtienen en los bordes ascendentes de la señal de pulso periódico externo, es decir, que a veces t es satisfactorio $f_{slow\ center}\left(\frac{x_{1(t)}}{2x_{1\ max}} + 1\right) t mod 2\pi = 0$. Hemos verificado numéricamente que, para las frecuencias de alta frecuencia f_{fast}, el efecto de ΔT se hace insignificante y el valor medio de la secuencia de bits de salida del $S_{(doble\ oscilador)}$ se acerca al ciclo de trabajo del reloj rápido.

De acuerdo con la ecuación 2 dada, se han generado secuencias binarias para diferentes coeficientes de centros de frecuencia f_{fast} y f_{slow} (f-alta y f-baja). En conclusión, hemos verificado numéricamente que el $S_{(doble\ oscilador)}$ de secuencia de bits, pasó las pruebas del conjunto de pruebas FIPS-140-2 sin el procesamiento de Von Neumann, hasta $\frac{f_{fast}}{f_{slow\ center}}$ = 40. En la figura 4, cómo puede aproximarse la entropía aproximada *ApEn* [17], del orden 8 para una longitud de secuencia de 20000 bit, la entropía de información máxima (*ln2*) que podría ser posible para un TRNG perfecto se mostró como una función de $\frac{f_{fast}}{f_{slow\ center}}$. Como se muestra en la figura 4 $\frac{f_{fast}}{f_{slow\ center}}$ = 200 es un valor óptimo para la relación dada, luego de lo cual *ApEn* no cambia tanto. Como resultado, para obtener secuencias binarias perfectamente no correlacionadas con entropía máxima, la frecuencia de f_{fast} debe aumentarse considerando un ciclo de trabajo equilibrado.

Debido a la falta de acceso a una instalación de fabricación adecuada, hemos elegido construir las innovaciones propuestas utilizando componentes discretos para mostrar la viabilidad de los circuitos y también hemos generado experimentalmente secuencias de bits. En el ejemplo, la arquitectura del doble oscilador se explota con

el oscilador caótico como se muestra en la figura 5. Dicho circuito se conoce a partir del documento *"A Truly Random Number Generator Based on a Continuous-Time Chaotic Oscillator for Applications in Cryptography"* ("Un generador de números verdaderamente aleatorios basado en un oscilador caótico de tiempo continuo para aplicaciones en criptografía") de SALIH ERGÜN *et al.*, COMPUTER AND INFORMATION SCIENCES - ISCIS 2005, LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER-VERLAG, BE, vol. 3733, 2005, págs. 205-214. En el circuito de ejemplo, 74HCT4046A VCO se usa para implementar la modulación de la frecuencia de reloj más lenta con la tensión v_1, que corresponde a la variable x_1. La frecuencia central del VCO determina la frecuencia central del reloj más lento.

Tal y como se explicó anteriormente, para eliminar la polarización de la secuencia de bits de salida, el oscilador rápido debería tener un ciclo de trabajo equilibrado. Para obtener un resultado satisfactorio, el oscilador rápido se implementa dividiendo un oscilador de cristal f_{fast}MHz de baja fluctuación por N dentro del FPGA. De esta forma, obtendremos un oscilador rápido f_{fast}MHz que tiene un ciclo de garantía del 50%.

Se diseñó un equipo basado en FPGA, que tiene una interfaz PCI para cargar los datos binarios en la computadora. La velocidad máxima de almacenamiento de datos de nuestro equipo basado en FPGA es de 62 Mbps. De acuerdo con el modelo numérico, el valor adecuado de $\frac{f_{fast}}{f_{slow\ center}}$ se determina en 200 y obtenemos resultados satisfactorios de forma experimental a partir del conjunto completo de pruebas NIST cuando la frecuencia de reloj más lenta se ajusta hasta 25 veces la frecuencia de operación central del oscilador caótico f_0. Luego, se muestrea el oscilador rápido en el borde ascendente del reloj más lento usando un *flip-flop* D o un flip-flop T dentro del FPGA. El nivel típico de desviación alta alcanzado por el oscilador modulado por caos para el circuito se muestra en la figura 6. El período mínimo medido y el período máximo, presentan una desviación estándar mucho mayor que el período del oscilador rápido, por lo tanto, proporciona flujo de bits aleatorio no correlacionado.

Además, se adquirió una secuencia de bits de 2 GB de longitud a través de la interfaz PCI del equipo basado en FPGA sin el procesamiento de Von Neumann. La frecuencia de reloj más lenta, que determina la velocidad de transmisión de datos, está básicamente limitada por el ancho de banda de la tensión v_1 y puede ajustarse hasta 25 f_0 para obtener resultados de prueba satisfactorios. Aunque la frecuencia del oscilador rápido es de 200 $f_{slow\ center}$, si se puede garantizar un ciclo de trabajo equilibrado, esta frecuencia debería aumentarse.

Finalmente, los bits obtenidos se sometieron a un conjunto completo de pruebas de NIST. Como resultado, hemos verificado experimentalmente que los datos binarios obtenidos mediante esta técnica de muestreo por oscilador pasaron las pruebas del conjunto completo de pruebas de números aleatorios NIST sin el procesamiento de Von Neumann para una mayor velocidad de rendimiento en comparación con los diseños de RNG anteriores basados en las otras técnicas. Los valores P fueron uniformes y la proporción de secuencias pasantes fue mayor que la tasa de aprobación mínima para cada prueba estadística.

La velocidad de datos de rendimiento del $S_{(doble\ oscilador)}$ se puede estimar como $S_{(doble\ oscilador)} \approx \frac{4}{\tau}$ en donde τ es la constante de tiempo del oscilador caótico. Podemos deducir que los osciladores caóticos pueden integrarse fácilmente en el proceso actual con una frecuencia central nominal en el rango de GHz. Sin embargo, debe notarse que los circuitos caóticos que operan a frecuencias mucho más altas ya se muestran en la literatura. Por ejemplo, los resultados de simulación de cadencia de la versión BJT de un oscilador caótico que opera a 5,3GHz se presentan en [18]; lo que da como resultado un rendimiento del orden de unos pocos cientos de Gbit/s.

Cabe señalar que en la innovación propuesta, el reloj más lento con fluctuaciones o caos-modulado se reemplaza por un comparador dando un tratamiento adecuado a las compensaciones.

Como se muestra en la figura 7, la secuencia binaria aleatoria S_{CDOA} se genera muestreando la salida de un oscilador rápido, en los bordes ascendente y/o descendente de la salida del comparador donde una de la señal, que corresponde a uno de los estados (x1 , x2, ... o xn) del oscilador caótico de tiempo continuo, se compara con un voltaje de umbral. Teniendo en cuenta las ventajas y desventajas de este enfoque, el primer pro del diseño basado en el comparador es la complejidad reducida, que se deriva del hecho de que un comparador puede implementarse usando estructuras simples en IC en comparación con la implementación de VCO y CCO. Una segunda ventaja de usar este diseño basado en el comparador es la capacidad de reducir la relación $\frac{f_{fast}}{f_{slowcenter}}$, que se determinó en 200 como en las secciones anteriores, hasta 1. En la figura 8 cómo la entropía aproximada *ApEn*, del orden 8 para una longitud de secuencia de 20 000 bit, se puede acercar a la entropía de información máxima (*ln2*) que podría ser posible para un TRNG perfecto se mostró como una función de $\frac{f_{fast}}{f_{slowcenter}}$, en donde $f_{slow\ center} = f_0$. Como se muestra en la figura 8, para f_0 = 1, 5, 10, 50, 100, 500, m = $\frac{f_{fast}}{f_{slowcenter}}$ = 0,15 es un valor óptimo para la relación dada, luego de lo cual *ApEn* no cambia tanto. Aunque m = 1 es una razón factible, para obtener secuencias binarias perfectamente desvinculadas con entropía máxima, la frecuencia de f_{fast} debe aumentarse considerando un ciclo de trabajo equilibrado.

Además de los pros, también hay contras de este enfoque. El enfoque basado en el comparador no ofrece el

mismo nivel de flexibilidad que la arquitectura de doble oscilador modulado por caos. La velocidad de datos de rendimiento de la arquitectura de doble oscilador basado en el comparador S_{CDOA}, se convierte efectivamente en $0,5f_0$ mientras que era 25 f_0 para la arquitectura de doble oscilador modulada por caos.

Además, el enfoque basado en el comparador también se puede aplicar en la arquitectura de doble oscilador clásico donde se usa una fuente de ruido para modular la frecuencia del reloj más lento. Como se muestra en la figura 9, el circuito de aplicación contiene un comparador, en lugar de un VCO o un CCO. En los bordes ascendentes y/o descendentes de este comparador, se genera una secuencia binaria aleatoria muestreando la salida del oscilador rápido mientras se compara el voltaje de ruido con un voltaje umbral.

Teniendo en cuenta el intercambio entre el rendimiento y la simplicidad, el uso del caos de tiempo continuo con las innovaciones propuestas es muy prometedor en la generación de números aleatorios con resultados muy elevados. Como resultado, los procedimientos propuestos son arquitecturas mejoradas donde se utiliza la arquitectura de doble oscilador con el oscilador caótico para maximizar la calidad estadística y el rendimiento de la secuencia de salida y para ser resistente contra interferencias externas, variaciones de parámetros y ataques dirigidos a forzar el rendimiento.

APLICACIÓN INDUSTRIAL

1. Generador de números verdaderamente aleatorios basado en un oscilador caótico autónomo para aplicaciones en criptografía

En el diseño propuesto, hemos obtenido datos aleatorios mediante el uso de la arquitectura de doble oscilador con el oscilador caótico para aumentar el rendimiento de salida y la calidad estadística de las secuencias de bits generadas. En este diseño, la señal de salida del oscilador caótico se usa para modular la frecuencia de un reloj más lento. Luego, con el borde ascendente del reloj más lento modulado por el caos, se muestrea el reloj rápido. Hemos desarrollado un modelo numérico para el diseño propuesto y finalmente hemos verificado de forma numérica y experimental que los datos binarios obtenidos por esta técnica de muestreo de oscilador pasaron las pruebas utilizadas tanto en el conjunto de pruebas FIPS-140-2 como en el conjunto de pruebas completa de números aleatorios NIST para una mayor velocidad de procesamiento.

2. Oscilador caótico autónomo

El oscilador caótico autónomo que se utiliza como núcleo del RNG se propuso en [18]. El oscilador caótico MOS se presenta en la figura 10 y se deriva del clásico oscilador sinusoidal acoplado mediante la adición de una sección RC_3 y una etapa de par diferencial (M_3 - M_4). Los pares de transistores M_9-M_8 y M_{10}-M_{11} se utilizan para implementar espejos de corriente simples con una relación de transferencia de corriente de k. Suponiendo que $C_1 = C_2 = C_3 = C$, el análisis de rutina del circuito produce la siguiente ecuación 3:

$$\begin{aligned}
&C(\dot{v_{C2}} - \dot{v_{C1}}) = \tfrac{\beta}{2}(v_{C2} - v_{C1})[(v_{C2} + v_{C1}) - 2V_{TH}] - \Delta i_L \\
&L\Delta\dot{i}_L = v_{C2} - v_{C1} - v_{C3} \\
&C(\dot{v_{C2}} + \dot{v_{C1}}) = kI_0 - I_B - \tfrac{\beta}{4}[(v_{C2} + v_{C1} - 2V_{TH})^2 + (v_{C2} - v_{C1})^2] \\
&2C\dot{v_{C3}} = \Delta i_L - \tfrac{2v_{C3}}{R} + k\begin{cases} I_0 & if\ v_{C2} - v_{C1} \geq V_{sat} \\ g_m(v_{C2} - v_{C1})\sqrt{1 - (\frac{v_{C2} - v_{C1}}{\sqrt{2}V_{sat}})^2} & if\ |v_{C2} - v_{C1}| < V_{sat} \\ -I_0 & if\ v_{C2} - v_{C1} \leq -V_{sat} \end{cases}
\end{aligned} \tag{3}$$

donde $\Delta i_L = i_L - i_R$ (corriente de inductores diferenciales), $g_m = \sqrt{\beta I_0},\ V_{sat} = \sqrt{\frac{2I_0}{\beta}},\ \beta = \mu_n C_{ox}(\frac{W}{L})_{1,2}$, V_{TH} es el voltaje umbral NMOS, μ_n es la movilidad electrónica, C_{ox} es la capacidad de óxido MOS y $\frac{W}{L}$ es la relación de aspecto de los pares de transistores M_1-M_2.

Usando las cantidades normalizadas: $R \equiv \sqrt{L/C},\ x_1 = \frac{v_{C2} - v_{C1}}{2V_{ref}},\ x_2 = \frac{v_{C2} + v_{C1}}{2V_{ref}},\ y = \frac{\Delta i_L R}{2V_{ref}},\ z = \frac{v_{C3}}{2V_{ref}}$, $t_n = t/RC$, y tomando $V_{ref} = V_{TH}$, las ecuaciones del sistema de la ecuación 3 se transforman en:

$$\begin{aligned}
&\dot{x_1} = bx_1(x_2 - 1) - y \\
&\dot{y} = x_1 - z \\
&\dot{x_2} = d - \tfrac{b}{2}[(x_2 - 1)^2 + x_1^2] \\
&2\dot{z} = y - 2z + k\begin{cases} c & if\ x_1 \geq x_{sat} \\ \sqrt{2bc}x_1\sqrt{1 - (\frac{x_1}{\sqrt{2}x_{sat}})^2} & if\ |x_1| < x_{sat} \\ -c & if\ x_1 \leq -x_{sat} \end{cases}
\end{aligned} \tag{4}$$

en donde b = βRV_{TH}, C= $\frac{I_0 R}{2V_{TH}}$, d = $\frac{(kI_0 - I_B)R}{2V_{TH}}$, y $x_{sat} = \frac{V_{sat}}{2V_{TH}} = \sqrt{\frac{c}{b}}$.

Las ecuaciones en 4 generan caos para diferentes conjuntos de parámetros. Por ejemplo, el atractor caótico que se muestra en la figura 11 se obtiene del análisis numérico del sistema con *b* = 0,9; *c* = 0,15; *d* = 0,7 y *k* = 8 usando un algoritmo *Runge-Kutta* de cuarto orden con un tamaño de paso adaptativo.

El oscilador caótico explotado ofrece algunas ventajas considerables sobre los existentes. El circuito emplea un par diferencial para realizar la no linealidad requerida, que es el bloque de construcción analógico básico más utilizado debido a su alto rendimiento de IC. Además, el oscilador caótico está equilibrado; por lo tanto, ofrece mejor rechazo de la fuente de alimentación e inmunidad al ruido.

3. Simulación de circuito

Para mostrar la capacidad de operación de alta frecuencia del oscilador caótico MOS, la disposición del circuito mostrado en la figura 10 se ha dibujado usando circuitos *Cadence* y *post-layout* (circuito post-diseño) y se ha simulado utilizando SPICE (*Nivel 3*) con el modelo de parámetros del proceso CMOS de 1,5µ. El circuito estaba polarizado con una fuente de alimentación de ± 2,5V. Los valores de componentes pasivos fueron: L = 4,7µH, C = 4,7pF, $(f_0 = \frac{1}{2\pi\sqrt{LC}} \approx 33.9MHz)$, R = 1000Ω y las corrientes de polarización fueron I_0 = 240μA, I_B = 100$_{\mu A}$, respectivamente. El espacio de fase observado correspondiente a v_{C2} - v_{C1} frente a v_{C3} se muestra en la figura 12.

Está claro que esta versión MOS del oscilador caótico requiere inductores sin chip. Intentar reducir los valores del inductor mientras se mantiene la funcionalidad no fue posible sin aumentar las tensiones de suministro, las corrientes de polarización y las relaciones de aspecto del transistor. Sin embargo, un similar atractor caótico también se obtuvo mediante el uso de la simulación SPICE con *L* = 20nH, *C* = 0,3pF, (f_0 ≈ 2GHz), *R* = 258Ω y con los parámetros del modelo de 0,35µ BiCMOS mientras que los voltajes de suministro fueron ± 2,5V y Las corrientes de polarización fueron I_0 = 1300µA, I_B = 400µA. Finalmente, el circuito del oscilador caótico es muy adecuado para la implementación monolítica y es capaz de operar a frecuencias muy altas.

4. Generación de números aleatorios

Debido a su extrema sensibilidad a las condiciones iniciales y al tener un exponente de Lyapunov positivo y un espectro de potencia similar al ruido, los sistemas caóticos se prestan para que sean explotados para la generación de números aleatorios. Para obtener datos binarios aleatorios de un sistema caótico de tiempo continuo, hemos presentado una técnica interesante, que se basa en generar datos binarios no invertibles a partir de la forma de onda del oscilador caótico dado. Cabe señalar que la no inversión es una característica clave para generar PRNG.

Para obtener bits aleatorios binarios del atractor caótico, usamos los valores del estado x_1 del sistema en la ecuación 4. Obsérvese que, aunque las trayectorias 4-dimensionales en el plano x_1-*y*-x_2-*z* son invertibles, se puede obtener una sección no invertible considerando solamente los valores correspondientes a uno de los estados, digamos x_1. En este diseño, la salida de un oscilador rápido se muestrea en el borde ascendente del reloj más lento modulado por el caos usando un flip-flop D. Un oscilador controlado por voltaje (VCO) se usa para implementar la modulación de la frecuencia de reloj más lenta con la señal caótica que corresponde a la variable x_1. La frecuencia central del VCO determina la frecuencia central del reloj más lento. La deriva entre los dos osciladores proporciona generación de bits aleatorios para ser más robustos. Debido al fenómeno de alias no lineal asociado con el muestreo, la arquitectura de doble oscilador logra un mayor rendimiento y una mayor calidad estadística [8].

Además, se ha desarrollado un modelo numérico para el diseño propuesto que permite la estimación de la entropía de bits de salida como una función de los parámetros de diseño. Suponiendo que VCO tiene una función de transferencia lineal, la frecuencia f_{slow} del reloj más se puede calcular de acuerdo como se muestra en la ecuación 5:

$$f_{slow} = f_{slow\ center}\left(\frac{x_1}{2x_{1\ max}} + 1\right) \qquad (5)$$

en dónde $\frac{f_{slow}}{2} < f_{slow} < \frac{3f_{slow}}{2}$, para $-x_{1\ máx} < x_1 < x_{1\ máx}$. Entre los intervalos dados, el reloj más lento produce un valor de frecuencia de salida para cada valor x_1. Si se conocen las frecuencias de reloj más rápidas y más lentas, así como la diferencia de fase de inicio Δ*T*, la salida del oscilador rápido, muestreada en el borde ascendente del reloj más lento modulado por el caos, se puede predecir como se ilustra en la figura 13. Se puede mostrar que los datos binarios del $S_{(doble\ oscilador)}$ son los inversos del bit menos significativo de la relación entre los períodos totales del reloj más lento y el período del reloj rápido:

$$S_{(dual\ oscillator)i} = (\lfloor \frac{(\sum_{j=1}^{i} T_{slow\ j}) - \Delta T}{T_{fast}/2} \rfloor mod2)' \qquad (6)$$
$$T_{slow\ j} = \frac{x_{1\ max}}{\frac{f_{slow\ center}}{2}(x_{1j} + 2x_{1\ max})}$$

donde el reloj rápido tiene un ciclo de trabajo del 50% y los valores x_{1j} se obtienen en los bordes ascendentes de la señal de pulso periódico externo, es decir, a veces t que satisface $f_{slow\ center}(\frac{x_{1(t)}}{2x_{1\ max}} + 1)tmod2\pi = 0$. Hemos verificado numéricamente que, para las altas frecuencias f_{fast}, el efecto de ΔT se hace insignificante y el valor medio de la secuencia de bits de salida del $S_{(doble\ oscilador)}$ se acerca al ciclo de trabajo del reloj rápido.

Según la ecuación 6 dada, se han generado secuencias binarias para diferentes relaciones de f_{fast} y $f_{slow\ center}$. En conclusión, hemos verificado numéricamente que el $S_{(doble\ oscilador)}$ de secuencia de bits, pasó las pruebas del conjunto de pruebas FIPS-140-2 sin el procesamiento de Von Neumann, hasta $\frac{f_{fast}}{f_{slow\ center}} = 40$. En la figura 14, se ve cómo puede aproximarse la entropía aproximada *ApEn* [18], del orden 8 para una longitud de secuencia de 20000 bits, la entropía de información máxima (*In2*) que podría ser posible para un TRNG perfecto y se muestra como una función de $\frac{f_{fast}}{f_{slow\ center}}$. Como resultado, para obtener secuencias binarias perfectamente no correlacionadas con entropía máxima, la frecuencia de f_{fast} debe aumentarse considerando un ciclo de trabajo equilibrado.

5. Verificación experimental y realización de equipo de RNG

Hemos elegido construir el oscilador caótico y el RNG propuesto usando componentes discretos para mostrar la viabilidad de los circuitos. Para la figura 10, los valores de componentes pasivos fueron: L = 9mH, C = 10nF, R = 1000Ω, I_B = 100μA y I_0 = 250μA. Los transistores MOS y las fuentes actuales, que se realizaron utilizando espejos de corriente simples, se implementaron con los conjuntos de transistores CMOS LM4007. Se configuró k igual a 8 ajustando la relación de las resistencias de carga de espejo actuales. La frecuencia de operación central del oscilador caótico: $f_0 = \frac{1}{2\pi\sqrt{LC}}$, se ajustó a un valor de frecuencia baja como 16,77 KHz a propósito para proporcionar el circuito para que no se vea afectado por capacitancias parasitarias. El circuito fue polarizado con una fuente de alimentación de ± 5V y el atractor observado se muestra en la figura 15.

5.1. Arquitectura de doble oscilador

De acuerdo con el procedimiento explicado en la sección 4, hemos generado bits aleatorios mediante el uso de la arquitectura del doble oscilador con el oscilador caótico como se muestra en la figura 5. En este circuito, se usa 74HCT4046A VCO para implementar la modulación de la frecuencia de reloj más lenta con la tensión $v_1 = v_{C2} - v_{C1}$, que corresponde a la variable x1. La frecuencia central del VCO determina la frecuencia central del reloj más lento.

Como se explicó en la sección 4, para eliminar la polarización de la secuencia de bits de salida, el oscilador rápido debería tener un ciclo de trabajo equilibrado. Para obtener un resultado satisfactorio, el oscilador rápido se implementa dividiendo un oscilador de cristal de baja intensidad de 152MHz por N = 8 dentro del FPGA. De esta manera, obtenemos un oscilador rápido de 19 MHz que tiene un ciclo de trabajo garantizado del 50%.

Un equipo basado en FPGA, que tiene una interfaz PCI, fue diseñado para cargar los datos binarios en la computadora. La velocidad máxima de almacenamiento de datos de nuestro equipo basado en FPGA es de 62 Mbps. De acuerdo con el modelo numérico, el valor inicial de $\frac{f_{fast}}{f_{slow\ center}}$ se determina en 200 y experimentalmente obtenemos resultados exitosos del conjunto completo de pruebas NIST cuando la frecuencia de reloj más lenta se ajusta hasta 211 KHz. Luego, se muestra un oscilador rápido de 19 MHz en el borde ascendente del reloj más lento utilizando un flip-flop D dentro del FPGA. El alto nivel de desviación alcanzado por el oscilador modulado por caos para el circuito se muestra en la figura 16. El período mínimo medido de 3.255 μs y el período máximo de 8.360 μseg, presentan una desviación estándar mucho mayor que el período del oscilador rápido, por lo tanto proporciona corriente de bits aleatoria no correlacionada.

Además, se adquirió una corriente de bit de longitud 2013MBits a través de la interfaz PCI del equipo basado en FPGA sin procesamiento de Von Neumann. La frecuencia de reloj más lenta, que determina la velocidad de transmisión de datos, está básicamente limitada por el ancho de banda de la tensión v_1 y puede ajustarse hasta 211 KHz para obtener resultados de prueba satisfactorios. Aunque la frecuencia del oscilador rápido es de 19 MHz, si se pudiera garantizar un ciclo de trabajo equilibrado, esta frecuencia debería aumentarse.

Finalmente, los bits obtenidos se sometieron a un conjunto completo de pruebas de NIST y hemos verificado experimentalmente que los datos binarios obtenidos por esta técnica de muestreo de oscilador superan las pruebas del conjunto completo de pruebas de NIST sin el procesamiento de Von Neumann para una mayor velocidad de rendimiento. Los resultados correspondientes para la uniformidad de los valores p y la proporción

de secuencias pasantes de la arquitectura del doble oscilador se muestran en la tabla 1. Se indica que, para un tamaño de muestra de 335 × 1M Bits, la tasa de aprobación mínima para cada estadística prueba con la excepción de la prueba de excursión aleatoria (variante) es aproximadamente 0,973691.

Al usar un oscilador caótico de tiempo continuo con una frecuencia central en el rango de GHz como el núcleo del RNG, la velocidad de datos de rendimiento de la arquitectura del doble oscilador, que se determinó como 221 KHz, puede ser probablemente mayor. En la sección 3, presentamos los resultados de la simulación del circuito post-diseño, lo que lleva a una frecuencia de operación central en (f_0 ≈ 33,9MHz). Teniendo en cuenta que el circuito se realizó en el proceso BiCMOS de 0,35μ como se indica en la Sección 3 (f_0 ≈ 2GHz), podemos deducir que el oscilador caótico puede integrarse fácilmente en el proceso actual con una frecuencia central nominal en el rango de GHz. Sin embargo, debe notarse que los circuitos caóticos que operan a frecuencias mucho más altas se informan en la literatura. Por ejemplo, los resultados de simulación de cadencia de la versión BJT del mismo oscilador caótico que opera a 5,3GHz se presentan en [18]. Por lo tanto, todo esto indica que el uso del caos de tiempo continuo es muy prometedor en la generación de números aleatorios con un rendimiento muy alto, del orden de decenas de Gbps.

Tabla 1: Resultados del conjunto de pruebas NIST para RNG usando arquitectura de doble oscilador con un oscilador caótico autónomo.

PRUEBAS ESTADÍSTICAS	$S_{doble\ oscilador}$	
	P - valor	Proporción
Frecuencia	0,373012	0,9881
Frecuencia de bloque	0,251604	0,9821
Sumas acumuladas	0,599316	0,9881
Carrera	0,008595	0,9791
Carrera más larga	0,279886	0,9881
Rango	0,247746	0,9881
FFT	0,324180	0,9940
Plantillas no periódicas	0,913396	1,0000
Plantillas superpuestas	0,712343	0,9940
Universal	0,531095	0,9881
Apen	0,706149	0,9940
Excursiones aleatorias	0,549331	0,9951
Variaciones de excursiones aleatorias	0,580051	1,0000
Serie	0,928429	0,9970
Complejidad lineal	0,275709	0,9851

6. Generadores de números realmente aleatorios basados en un atractor de doble desplazamiento

En el diseño propuesto, hemos obtenido datos aleatorios mediante el uso de la arquitectura de doble oscilador con el oscilador caótico para aumentar el rendimiento de salida y la calidad estadística de las secuencias de bits generadas. En este diseño, la señal de salida del oscilador caótico se usa para modular la frecuencia de un reloj más lento. Luego, con el borde ascendente del reloj más lento modulado por el caos, se muestrea el reloj rápido. Finalmente, hemos verificado experimentalmente que los datos binarios obtenidos por esta técnica de muestreo de oscilador pasan las pruebas de conjunto completo de pruebas de números aleatorios NIST para una velocidad de procesamiento mayor que la obtenida mediante el uso de un oscilador caótico por sí solo.

7. Atractor de doble desplazamiento

El atractor de doble desplazamiento que se utiliza como núcleo del RNG se obtiene a partir de un modelo simple mostrado en [22], que se expresa mediante la ecuación 7. Debe observarse que cuando la no linealidad se reemplaza por una continua la no linealidad, el sistema es "cualitativamente similar" al oscilador de Chua.

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= z \\ \dot{z} &= -ax - ay - a\dot{z} + sgn(x) \end{aligned} \qquad (7)$$

Las ecuaciones en 7 generan caos para diferentes conjuntos de parámetros. Por ejemplo, el atractor caótico que se muestra en la figura 17 se obtiene del análisis numérico del sistema con *a* = 0,666 usando un algoritmo Runge-Kutta de cuarto orden con un tamaño de paso adaptativo.

8. Generación aleatoria de bits

Para obtener datos binarios aleatorios de un sistema caótico de tiempo continuo, hemos presentado una técnica interesante, que se basa en generar datos binarios no invertibles de la forma de onda del sistema caótico dado. Cabe señalar que la no inversión es una característica clave para generar PRNG. Propusimos un nuevo diseño RNG que utiliza una arquitectura de doble oscilador con el oscilador caótico. En este diseño, la salida de un oscilador rápido se muestrea en el borde ascendente del reloj más lento modulado por el caos usando un flip-flop D. Se podría usar un oscilador controlado por voltaje (VCO) para implementar la modulación de la frecuencia de reloj más lento con la señal de salida del oscilador caótico. La frecuencia central del VCO determina la frecuencia central del reloj más lento. La deriva entre los dos osciladores proporciona generación de bits aleatorios que son más robustos. Debido al fenómeno de alias no lineal asociado con el muestreo, la arquitectura del doble oscilador logra un mayor rendimiento y una mayor calidad estadística. Se ha indicado que para obtener un flujo de bits aleatorio no correlacionado, el período del oscilador lento más modulado debería presentar una desviación estándar mucho mayor que el período del oscilador rápido. Aunque no hemos analizado numéricamente la arquitectura del doble oscilador, hemos verificado experimentalmente que los datos binarios, obtenidos mediante esta técnica de muestreo por oscilador, pasan las pruebas del conjunto completo de pruebas NIST sin el procesamiento de Von Neumann para una mayor velocidad de procesamiento.

9. Realización de equipo de RNG

Hemos elegido construir el circuito propuesto utilizando componentes discretos para mostrar la viabilidad del circuito.

El circuito estaba polarizado con una fuente de alimentación de ± 5V. El diagrama de circuito que realiza el atractor de doble desplazamiento se muestra en la figura 18. Se utiliza AD844 como un amplificador operacional de alta velocidad y el comparador de voltaje LM211 se usa para realizar la no linealidad requerida. Los valores de componentes pasivos se tomaron como: $R_1 = R_2 = aR_3 = R = 10k\Omega$, $R_3 = 15k\Omega$ para $a = 0,666$; $C_{17} = C_{18} = C_{19} = C = 2,2nF$ y $R_K = 100k\Omega$.

Por lo tanto, la frecuencia principal del oscilador caótico: $f = \frac{1}{2\pi\tau}$ correspondiente a la constante de tiempo τ donde τ = RC, se ajustó a propósito a un valor de baja frecuencia como 7,234 KHz para proporcionar que el circuito no se viera afectado por capacitancias parasitarias. El atractor observado se muestra en la figura 19.

9.1 Arquitectura de doble oscilador

En el ejemplo, la arquitectura del doble oscilador se explota con el oscilador caótico como se muestra en la figura 5. En este circuito, 74HCT4046A VCO se usa para implementar la modulación de la frecuencia de reloj más lenta con la tensión v_1, que corresponde a la variable x. La frecuencia central del VCO determina la frecuencia central del reloj más lento.

Para eliminar la polarización de la secuencia de bits de salida, el oscilador rápido debería tener un ciclo de trabajo balanceado. Para obtener un resultado satisfactorio, el oscilador rápido se implementa dividiendo un oscilador de cristal de baja intensidad de 152MHz por N = 8 dentro del FPGA. De esta manera, obtenemos un oscilador rápido de 19 MHz que tiene un ciclo de trabajo garantizado del 50%.

Se diseñó un equipo basado en FPGA, que tiene una interfaz PCI para cargar los datos binarios en la computadora. La velocidad máxima de almacenamiento de datos de nuestro equipo basado en FPGA es de 62 Mbps. Los osciladores rápidos y lentos utilizados en [1] y [9] tienen ratios de frecuencia central del orden de 1: 100. En nuestro diseño, obtenemos resultados experimentales de forma exitosa de la suite completa de pruebas NIST cuando la frecuencia de reloj más lenta se ajusta hasta 170 kHz Luego, se muestra un oscilador rápido de 19 MHz en el borde ascendente del reloj más lento utilizando un flip-flop D dentro del FPGA. En la figura 20 se muestra una instantánea del osciloscopio que muestra el alto nivel de desviación alcanzado por el oscilador modulado por caos para el circuito. El período mínimo medido 3,875 µsec y el período máximo 13,468 µsec, presentan una desviación estándar mucho mayor que el período del oscilador rápido, por lo tanto, proporciona un flujo de bits aleatorio no correlacionado. Además, se adquirió un flujo de bits de 24,2 GB de longitud a través de la interfaz PCI del equipo basado en FPGA sin el procesamiento de Von Neumann. La frecuencia de reloj más lenta, que determina la velocidad de transmisión de datos, está básicamente limitada por el ancho de banda de la tensión v_1 y puede ajustarse hasta 170 KHz para obtener resultados de prueba satisfactorios. Aunque la frecuencia del oscilador rápido es de 19 MHz, si se puede garantizar un ciclo de trabajo equilibrado, esta frecuencia debería aumentarse.

Finalmente, los bits obtenidos se sometieron a un conjunto completo de pruebas NIST y hemos verificado

experimentalmente que los datos binarios obtenidos mediante esta técnica de muestreo por oscilador superan las pruebas del conjunto completo de pruebas NIST sin el procesamiento de Von Neumann para una mayor velocidad de procesamiento. Los resultados de las pruebas correspondientes se dan en la tabla 2. Las tasas mínimas de aprobación para cada prueba estadística con la excepción de la prueba de excursión aleatoria (variante) para RNG usando la arquitectura de doble oscilador también se muestran en la primera línea de la tabla 2.

En [22], una realización de chip del sistema de doble desplazamiento con una frecuencia central de operación en $f = \frac{1}{2\pi\tau_{new}}$ = 500 *KHz* ha sido presentado. Teniendo en cuenta que el circuito en [22] se realizó en un proceso relativamente lento de 1,2u CMOS, podemos deducir que el circuito se puede integrar fácilmente en el proceso de hoy en un par de 10MHz. Sin embargo, debe notarse que en la literatura se informan los circuitos caóticos que funcionan a frecuencias mucho más altas. Por ejemplo, los resultados de simulación de cadencia de un circuito caótico que opera a 5,3GHz se presentan en [18]. Al usar un oscilador caótico de tiempo continuo con una frecuencia principal mayor que el núcleo del RNG, la tasa de datos de rendimiento de la arquitectura de doble oscilador, que se determinó como 170 KHz, probablemente sea más alta que la tasa indicada anteriormente.

Tabla 2: Resultados de la suite de pruebas NIST para RNG usando arquitectura de doble oscilador con un atractor de doble desplazamiento.

PRUEBAS ESTADÍSTICAS	*Secuencia bits* $S_{doble\ oscilador}$
Tasas mínimas de pases	0,9736
Frecuencia	0,9940
Frecuencia de bloque	0,9940
Sumas acumuladas	0,9925
Carrera	0,9940
Carrera más larga	0,9881
Rango	0,9881
FFT	0,9970
Plantillas no periódicas	0,9895
Plantillas superpuestas	0,9821
Universal	0,9881
Apen	0,9851
Excursiones aleatorias	0,9914
Variaciones de excursiones aleatorias	0,9900
Serie	0,9895
Complejidad lineal	0,9761

10. Generadores de números realmente aleatorios basados en caos de tiempo continuo

A pesar del hecho de que, el uso de mapas caóticos de tiempo discreto en la realización de RNG ha sido bien conocido durante bastante tiempo, recientemente se demostró que los osciladores caóticos de tiempo continuo también pueden usarse para realizar TRNG. Siguiendo en esta dirección, investigamos la utilidad de los osciladores caóticos propuestos como núcleo de un RNG.

Aunque existen muchos osciladores caóticos en la literatura, solo algunos de ellos han sido diseñados teniendo en cuenta los problemas del diseño de un IC de alto rendimiento, tales como bajo consumo de energía, operación de alta frecuencia, capacidad de operación a bajos niveles de voltaje. En este trabajo, presentamos osciladores caóticos simples no autónomos, que son adecuados para la realización de un IC de alto rendimiento.

Hemos propuesto un diseño de RNG que utiliza una arquitectura de doble oscilador con el oscilador caótico propuesto para aumentar el rendimiento de salida y la calidad estadística de las secuencias de bits generadas. En este diseño, la señal de salida del oscilador caótico se usa para modular la frecuencia de un reloj más lento. Luego, con el borde ascendente del reloj más lento modulado por el caos, se muestrea el reloj rápido. Finalmente, hemos verificado experimentalmente que los datos binarios obtenidos por esta técnica de muestreo de oscilador pasaron las pruebas del conjunto completo de pruebas de números aleatorios NIST para una

velocidad de procesamiento mayor que la obtenida usando solo el oscilador caótico continuo.

11. Osciladores propuestos

El oscilador caótico bipolar propuesto se presenta en la figura 21. Suponiendo que las capacitancias parasitarias que aparecen entre los colectores de los transistores bipolares y la tierra se denotan por C_p, el análisis de rutina del circuito produce las siguientes ecuaciones de estado:

$$\begin{aligned} C\dot{v}_1 &= -i_3 \\ L\dot{i}_3 &= (v_1 - v_2) \\ C_p\dot{v}_2 &= i_3 - (\tfrac{1}{R} + \tfrac{1}{R_p})v_2 + \tfrac{2}{R_p}V_p sgn(sin\Omega t) + \\ &\quad I_0 tanh(v_1/2V_T) \end{aligned} \tag{8}$$

en donde $i_3 = i_R - i_L$ y $u_p(t)$ es el tren de impulsos periódico externo definido como $vp(t) = sgn(sin\Omega t)$ y V_T es el voltaje térmico ($V_T = kT/q$), que es igual a 25,8mV a temperatura ambiente.

Usando las cantidades normalizadas: $R_0 \equiv \sqrt{L/C}$ $x = v_1/V_s$, $y = i_3R_0/V_s$, $z = v_2/V_s$, $c_0 = I_0R_0/V_s$, $\alpha = R_0/R_p$, $\beta = R_0/R$, $\omega \equiv \Omega\sqrt{LC}$, y tomando $V_p = 0{,}5V_s = V_T$ y $t_n = t/RC$, donde V_S es un voltaje de escala arbitrario, las ecuaciones del sistema en la ecuación 8 se transforma en:

$$\begin{aligned} \dot{x} &= -y \\ \dot{y} &= x - z \\ \epsilon\dot{z} &= y - (\alpha + \beta)z + \alpha sgn(sin\omega t) + c_0 tanh(x) \end{aligned} \tag{9}$$

Las ecuaciones en 9 generan caos para diferentes conjuntos de parámetros. Por ejemplo, el atractor caótico que se muestra en la figura 22 se obtiene del análisis numérico del sistema con $c_0 = 25$, $\alpha = 4$, $\beta = 12$, $\omega = 0.27$, $\varepsilon = 0{,}3$ utilizando un algoritmo Runge-Kutta de cuarto orden con un tamaño de paso adaptativo.

El oscilador caótico CMOS propuesto se presenta en la figura 23. Los pares de transistores T_3-T_4 y T_5-T_6 se utilizan para implementar espejos de corriente simples, donde las relaciones actuales de los espejos se indican por K. Suponiendo que las capacitancias parasitarias que aparecen entre las puertas de los pares de transistores T_1-T_2 y la tierra se denotan por C_p, el análisis de rutina del circuito produce la siguiente ecuación 10:

$$\begin{aligned} &C\dot{v}_1 = -i_3 \\ &L\dot{i}_3 = (v_1 - v_2) \\ &C_p\dot{v}_2 = i_3 - (\tfrac{1}{R} + \tfrac{1}{R_p})v_2 + \tfrac{2}{R_p}V_p sgn(sin\Omega t) \\ &+K\begin{cases} I_0 & if\ V_{G1} - V_{G2} \geq \sqrt{2}V_{sat} \\ g_m(V_{G1} - V_{G2})\sqrt{1 - (\frac{V_{G1} - V_{G2}}{2V_{sat}})^2} & if\ \sqrt{2}V_{sat} > V_{G1} - V_{G2} \geq -\sqrt{2}V_{sat} \\ -I_0 & if\ V_{G1} - V_{G2} < -\sqrt{2}V_{sat} \end{cases} \end{aligned} \tag{10}$$

en donde $i_3 = i_R - i_L$ y $v_p(t) = sgn(sin\Omega t)$, $g_m = \sqrt{\mu_n C_{ox}\frac{W}{L}I_0}$, $V_{sat} = \sqrt{\frac{I_0}{\mu_n C_{ox}\frac{W}{L}}}$ y $\frac{W}{L}$ es la relación ancho-longitud de los pares de transistores T_1-T_2.

Usando las cantidades normalizadas: $R_0 \equiv \sqrt{L/C}$ $x = V_{G1}/V_s$, $y = i_3R_0/V_s$, $z = V_{G2}/V_s$, $c_0 = 2I_0R_0/V_s$, $\alpha = R_0/R_p$, $\beta = R_0/R$, $b_0 = R_0\beta V_s/2$, $\omega \equiv \Omega\sqrt{LC}$ y tomando $V_p = 0{,}5V_s$, y, $t_n = t/RC$, donde V_S es un voltaje de escala arbitrario, las ecuaciones del sistema en la ecuación 10 se transforman en:

$$\begin{aligned} &\dot{x} = -y \\ &\dot{y} = x - z \\ &\epsilon\dot{z} = y - (\alpha + \beta)z + \alpha sgn(sin\omega t) + K\begin{cases} 0.5c_0 & if\ x \geq \sqrt{\frac{c_0}{2b_0}} \\ b_0 x\sqrt{\frac{c_0}{b_0} - x^2} & if\ \sqrt{\frac{c_0}{2b_0}} > x \geq -\sqrt{\frac{c_0}{2b_0}} \\ -0.5c_0 & if\ x < -\sqrt{\frac{c_0}{2b_0}} \end{cases} \end{aligned} \tag{11}$$

Las ecuaciones en 11 generan caos para diferentes conjuntos de parámetros. Por ejemplo, el atractor caótico que se muestra en la figura 24 se obtiene del análisis numérico del sistema con $c_0 = 1{,}5$, $\alpha = 2{,}67$, $\beta = 3{,}38$, $\omega = 0{,}33$, $b_0 = 0{,}9$, $\varepsilon = 0{,}1$ usando un algoritmo Runge-Kutta de cuarto orden con un tamaño de paso adaptativo.

Los osciladores caóticos propuestos ofrecen algunas ventajas considerables sobre los osciladores existentes.

Ambos circuitos emplean un par diferencial para realizar la no linealidad requerida, que es el bloque de construcción analógico básico más utilizado debido a su alto rendimiento de IC. Las resistencias empleadas en los circuitos tienen valores muy pequeños, por lo que pueden realizarse de manera efectiva en IC. Además, los osciladores caóticos propuestos están equilibrados; por lo tanto, ofrecen mejor rechazo de la fuente de alimentación e inmunidad al ruido. Finalmente, la fuente externa utilizada para conducir los circuitos es un tren de impulsos periódico, que puede realizarse con precisión y facilidad utilizando la señal de reloj ya disponible en el chip.

12. Mecanismo de generación de caos

Se sabe que las condiciones de Melnikov pueden usarse para mostrar la existencia de herraduras en sistemas disipadores planares forzados casi hamiltonianos. De acuerdo con el Teorema de Smale-Birkhoff, para un sistema planar perturbado no lineal dado de la forma, $\dot{x} = f(x) + \mu g(x, t)$, donde f y g son funciones suaves y g es periódico en el tiempo con un período de T_Y, si se cumplen las siguientes condiciones:

1. Para $\mu = 0$, el sistema es hamiltoniano y tiene una órbita homoclínica que pasa a través del punto crítico del tipo montura o sillín.

2. Para $\mu = 0$, el sistema tiene una familia de parámetros de órbitas periódicas $\theta_Y(t)$ del período T_Y en el interior de la órbita homoclínica con, $\partial\theta_Y(0)/\partial_Y \neq 0$.

3. Para $t_0 \in [0,T]$ La función Melnikov en la ecuación 12 tiene ceros simples.

$$M(t_0) = \int_{-\infty}^{+\infty} f^0(\tau) \wedge g^0(\tau + t_0) d\tau \qquad (12)$$

entonces el sistema tiene movimientos caóticos y herraduras.

Es fácil verificar que para $\varepsilon = 0$ (las capacitancias parasitarias se descuidan), el sistema en la ecuación 9 puede escribirse de la siguiente manera:

$$\begin{bmatrix} \dot{x} \\ \dot{y} \end{bmatrix} = \begin{bmatrix} -y \\ x - a\tanh x \end{bmatrix} + \mu \begin{bmatrix} 0 \\ -y - \alpha x_p(t) \end{bmatrix} \qquad (13)$$

en donde $x_p(t) = sgn(sin(\omega t))$, $a = c_0/(\alpha + \beta)$ y $\mu = 1/(\alpha+\beta)$. En este caso, se puede verificar fácilmente que el sistema no perturbado obtenido para μ = 0 tiene un punto crítico de tipo montura en el origen para a> 1. Además, el sistema no perturbado es hamiltoniano y tiene una órbita homoclínica que pasa por el punto crítico. Después de reemplazar la función no suave $x_p(t) = sgn(sin(\omega t))$ con su aproximación suave $x_p(t) = tanh(10sin(\omega t))$, calculamos numéricamente la función Melnikov dada en la ecuación 14:

$$M(t_0) = \int_{-\infty}^{+\infty} -y^0(y^0 + \alpha x_p(t + t_0)) d\tau \qquad (14)$$

en la órbita homoclínica de la ecuación 13 que se muestra en la esquina superior derecha de la figura 25. Como se muestra en la figura 25, hemos verificado que la función Melnikov tiene ceros simples para $t_0 \in [0, T]$ y el sistema en la ecuación 13 tiene movimientos caóticos y herraduras. El análisis numérico del sistema muestra que el sistema sigue siendo caótico para valores distintos de cero y pequeños. Por ejemplo, el mayor exponente de Lyapunov del sistema se encuentra en 0,9 para ε = 0,27.

13. Generación aleatoria de bits

Para obtener datos binarios aleatorios de un sistema caótico autónomo, se ha presentado una técnica interesante, que se basa en la generación de datos binarios no invertibles a partir de la forma de onda del sistema caótico dado. Cabe señalar que la no inversión es una característica clave para generar PRNG. Hay que tener en cuenta que, aunque la sección bidimensional en el plano x-y es invertible, se puede obtener un mapa no invertible considerando únicamente los valores correspondientes a uno de los estados, por ejemplo x. En el RNG propuesto, se utiliza la arquitectura de doble oscilador con los osciladores caóticos propuestos. En este diseño, la salida de un oscilador rápido se muestrea en el borde ascendente del reloj más lento modulado por el caos usando un flip-flop D. Un oscilador controlado por voltaje (VCO) se usa para implementar la modulación de la frecuencia de reloj más lenta con la señal de salida del oscilador caótico x. La frecuencia central del VCO determina la frecuencia central del reloj más lento. La deriva entre los dos osciladores proporciona una generación de bits aleatorios para que sean más robustos. Debido al fenómeno de alias no lineal asociado con el muestreo, la arquitectura del doble oscilador logra un mayor rendimiento y una mayor calidad estadística. Se ha

mostrado que para obtener un flujo de bits aleatorio no correlacionado, el período del oscilador lento más modulado debería presentar una desviación estándar mucho mayor que el período del oscilador rápido. Aunque no hemos analizado numéricamente la arquitectura del doble oscilador, hemos verificado experimentalmente que los datos binarios, obtenidos mediante esta técnica de muestreo por oscilador, pasan las pruebas del conjunto completo de pruebas NIST sin el procesamiento de Von Neumann para una mayor velocidad de procesamiento.

14. Verificación experimental

Hemos elegido construir los circuitos del oscilador caótico propuesto utilizando componentes discretos para mostrar la viabilidad de los circuitos. Ambos circuitos bipolares y CMOS se polarizaron con un único suministro de energía de 5V y la señal externa $v_p(t)$ fue generada por un generador de onda cuadrada.

Los valores de los componentes pasivos del oscilador bipolar fueron: $L = 10mH$, $C = 10nF$, $R = 180\Omega$, $R_p = 120\Omega$ e $I_0 = 1,2mA$. En la figura 21, los transistores bipolares y la fuente de corriente indicada por I_0, que se realizó utilizando un espejo de corriente simple, se implementaron con los conjuntos de transistores CA3046 y CA3096 NPN y PNP. La amplitud de $v_p(t)$ fue de 26 mV. Hemos verificado experimentalmente que el circuito bipolar propuesto tenía movimientos caóticos para los siguientes valores de frecuencia de $v_p(t)$ (5,95 KHz, 6,23 KHz, 7,12 KHz, 13,03 KHz, 14,48 KHz, 14,91 KHz, 17,07 KHz, 17,23 KHz, 18,08 KHz).

Los valores de los componentes pasivos del oscilador CMOS fueron: $L = 10mH$, $C = 10nF$, $R = 340\Omega$, $R_p = 430\Omega$ y $I_0 = 0,5mA$. En la figura 23, los transistores CMOS y la fuente actual indicada por I_0, que se realizó utilizando un espejo de corriente simple, se implementaron con matrices de transistores CMOS LM4007. La amplitud de $v_p(t)$ fue de 383mV. Hemos verificado experimentalmente que el circuito CMOS propuesto tenía movimientos caóticos para los siguientes valores de frecuencia de $v_p(t)$ (5,95 KHz, 10 KHz, 11,1 KHz, 12,6 KHz).

Para ambos osciladores bipolares y CMOS, la frecuencia de $v_p(t)$ se ajustó a un valor de baja frecuencia de 5,95 KHz a propósito para proporcionar que los circuitos que no se vieran afectados por capacitancias parasitarias. Los atractores observados se muestran en la figura 26 y en la figura 27 los osciladores bipolares y CMOS, respectivamente.

15. Realización de equipo de RNG

Hemos generado bits aleatorios mediante el uso de la arquitectura del doble oscilador con los osciladores caóticos como se muestra en la figura 5. En este circuito, de acuerdo con el procedimiento anterior, 74HCT4046A VCO se usa para implementar la modulación de la frecuencia de reloj más lenta con el voltaje v_1, que corresponde a la variable x. La frecuencia central del VCO determina la frecuencia central del reloj más lento.

Se diseñó un equipo basado en FPGA, que tiene una interfaz PCI para cargar los datos binarios en la computadora. La velocidad máxima de almacenamiento de datos de nuestro equipo basado en FPGA es de 62 Mbps. Para eliminar la polarización de la secuencia de bits de salida, el oscilador rápido debe tener un ciclo de trabajo balanceado. Para obtener un resultado satisfactorio, el oscilador rápido se implementa dividiendo un oscilador de cristal de baja intensidad de 152MHz por N = 8 dentro del FPGA. De esta manera, obtenemos un oscilador rápido de 19 MHz que tiene un ciclo de trabajo garantizado del 50%.

Los osciladores lentos y rápidos utilizados en [1] y [9] tienen coeficientes de frecuencia central del orden de 1: 100. En nuestro diseño, obtenemos resultados exitosos de forma experimental en el conjunto completo de pruebas de NIST cuando la frecuencia de reloj más lenta se ajusta hasta 1,81 MHz. Luego, se muestra un oscilador rápido de 19 MHz en el borde ascendente del reloj más lento utilizando un flip-flop D dentro del FPGA. El alto nivel de fluctuación alcanzado por el oscilador modulado por caos para el circuito CMOS se muestra en la figura 28. El período mínimo medido 610,927 ns y el período máximo 1001,024 ns presentan una desviación estándar mucho mayor que el período del oscilador rápido, por lo tanto proporciona una secuencia de bits aleatoria no correlacionada.

Además, para circuitos bipolares y CMOS, se obtuvo un flujo de bits de longitud de 4,83 GBytes a través de la interfaz PCI del equipo basado en FPGA sin procesamiento de Von Neumann. Los bits obtenidos se sometieron a un conjunto completo de pruebas NIST. Para diferentes valores de frecuencia de $v_p(t)$ de 5,95 KHz a 18,08 KHz para el circuito bipolar y de 5,95 KHz a 12,6 KHz para el circuito CMOS donde los osciladores propuestos generan caos como se mencionó anteriormente, hemos verificado experimentalmente que los datos binarios obtenidos por esta técnica de muestreo de osciladores pasa las pruebas de la suite completa de pruebas NIST. Las tasas de aprobación de las pruebas son aproximadamente las mismas para los valores de frecuencia dados de $v_p(t)$.

La frecuencia de $v_p(t)$ se ajusta a 5,95 KHz. Los resultados de las pruebas del circuito CMOS se muestran en la tabla 3 para tres valores de frecuencia diferentes del oscilador más lento cuando la frecuencia del oscilador rápido es de 19 MHz. La frecuencia de reloj más lenta, que determina la velocidad de transmisión de datos, está básicamente limitada por la frecuencia de voltaje v_1 y puede ajustarse hasta 1,81 MHz, como se muestra en la

tabla 3. Si se pudiera garantizar un ciclo de trabajo balanceado, debería incrementarse la frecuencia del oscilador rápido.

Como resultado, se presentaros los osciladores Bipolar y CMOS, como dos nuevos osciladores caóticos de tiempo continuo adecuados para la realización de IC y nuevos TRNG basados en estos osciladores. Los resultados experimentales presentados en esta sección no solo verifican la viabilidad de los circuitos propuestos, sino que también alientan su uso como el núcleo de un IC TRNG de alto rendimiento. En conclusión, hemos verificado experimentalmente que, cuando la frecuencia de la señal de pulso periódica externa se ajusta a 5,95 KHz, las velocidades de datos de rendimiento de las secuencias regionales son de 1,81 Mbps sin procesamiento de Von Neumann. Finalmente, hemos verificado experimentalmente que, para los circuitos bipolares y CMOS, los datos binarios obtenidos por esta técnica de muestreo de oscilador pasaron las pruebas de la suite completa de pruebas NIST sin el procesamiento de Von Neumann para una mayor velocidad de procesamiento, al tiempo que se comparan con los diseños de TRNG donde se utilizan los osciladores caóticos de tiempo continuo por sí solos.

Tabla 3: Resultados del conjunto de pruebas NIST para RNG usando arquitectura de doble oscilador con un oscilador caótico no autónomo. ($fv_p(t)$ = 5,95KHz, oscilador rápido $f_{fastoscillator}$ = 19MHz)

PRUEBAS ESTADÍSTICAS	$F_{slowoscillador}$		
	1.58 MHz	1.81 MHz	1.94 MHz
Frecuencia	0.9931	1.0000	0.9940
Frecuencia de bloque	0.9946	0.9881	0.9791
Sumas acumuladas	0.9911	0.9985	0.9925
Carreras	0.9839	0.9940	x
Carrera más larga	0.9821	0.9881	0.9851
Rango	0.9925	0.9910	0.9910
FFT	0.9991	1.0000	0.9940
Plantillas no periódicas	0.9882	0.9882	0.9802
Plantillas superpuestas	0.9848	0.9851	0.9433
Universal	1.0000	0.9970	0.9851
Apen	0.9779	0.9821	x
Excursiones aleatorias	0.9874	0.9870	0.9902
Variaciones de excursiones aleatorias	0.9906	0.9897	0.9880
Serie	0.9870	0.9746	0.9865
Lempel Ziv	0.9797	0.9821	0.9851
Complejidad lineal	0.9869	0.9881	0.9821

Referencias

[1] Jun, B., Kocher, P.: The Intel Random Number Generator. Cryptography Research, Inc., documentos técnicos preparados para Inter Corp. http://www.cryptography.com/resources/whitepapers/IntelIRNG.pdf (1999).

[2] Menezes, A., Oorschot, P.van, Vanstone, S.: Handbook of Applied Cryptology. CRC Press (1996).

[3] Schrift, A. W., Shamir, A.: On the Universality of the Next Bit Test. Proceeding of the CRYPTO. (1990) 394-408.

[4] Schneier, B.: Applied Cryptography. 2nd edn. John Wiley & Sons (1996).

[5] Holman, W.T., Connelly, J.A., Downlatabadi, A.B.: An Integrated Analog-Digital Random Noise Source. IEEE Trans. Circuits and Systems I, Vol. 44. 6 (1997) 521-528.

[6] Bagini, V., Bucci, M.: A Design of Reliable True Random Number Generator for Cryptographic Applications. Proc. Workshop Cryptographic Hardware and Embedded Systems (CHES). (1999) 204-218.

[7] Dichtl, M., Janssen, N.: A High Quality Physical Random Number Generator. Proc. Sophia Antipolis Forum Microelectronics (SAME). (2000) 48-53.

[8] Petrie, C.S., Connelly, J.A.: A Noise-Based IC Random Number Generator for Applications in Cryptography. IEEE Trans. Circuits and Systems I, Vol. 47. 5 (2000) 615-621.

[9] Bucci, M., Germani, L., Luzzi, R., Trifiletti, A., Varanonuovo, M.: A High Speed Oscillator-based Truly Random Number Source for Cryptographic Applications on a SmartCard IC. IEEE Trans. Comput. Vol. 52. (2003) 403-409.

[10] Stojanovski, T., Kocarev, L.: Chaos-Based Random Number Generators-Part I: Analysis. IEEE Trans. Circuits and Systems I, Vol. 48, 3 (2001) 281-288.

[11] Stojanovski, T., Pihl, J., Kocarev, L.: Chaos-Based Random Number Generators-Part II: Practical Realization. IEEE Trans. Circuits and Systems I, Vol. 48, 3 (2001) 382-385.

[12] Delgado-Restituto, M., Medeiro, F., Rodriguez-Vazquez, A.: Nonlinear Switched-current CMOS IC for Random Signal Generation. Electronics Letters, Vol. 29(25). (1993) 2190-2191.

[13] Callegari, S., Rovatti, R., Setti, G.: Embeddable ADC-Based True Random Number Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos. IEEE Transactions on Signal Processing, Vol. 53, 2 (2005) 793-805.

[14] Callegari, S., Rovatti, R., Setti, G.:First Direct Implementation of a True Random Source on Programmable Hardware. International Journal of Circuit Theory and Applications, Vol. 33 (2005) 1-16.

[15] Yalcin, M.E., Suykens, J.A.K., Vandewalle, J.: True Random Bit Generation from a Double Scroll Attractor. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 51(7). (2004) 1395-1404.

[16] National Institute of Standard and Technology, FIPS PUB 140-2, Security Requirements for Cryptographic Modules, NIST, Gaithersburg, MD 20899, (2001).

[17] National Institute of Standard and Technology.: A Statistical Test Suite for Random and Pseudo Random Number Generators for Cryptographic Applications. NIST 800-22, http://csrc.nist.gov/rng/SP800-22b.pdf (2001).

[18] Özoğuz, S., Ate, Ö., Elwakil, A.S.: An integrated circuit chaotic oscillator and its application for high speed random bit generation. Proceeding of the International Symposium on Circuit and Systems (ISCAS). (2005) 4345-4348.

[19] Shamir, A.: On The Generation of Cryptographically Strong Pseudorandom Sequences. ACM Transactions on Computer systems, Vol. 1. (1983) 38-44.

[20] Von Neumann, J.: Various Techniques Used in Connection With Random Digits. Applied Math Series - Notes by G.E. Forsythe, In National Bureau of Standards, Vol. 12. (1951) 36-38.

[21] Young, L.: Entropy, Lyapunov exponents and Hausdorff dimension in diffrentiable dynamical systems. IEEE Trans. Circuits Syst. I, Vol. 30. (1983) 599-607.

[22] Elwakil, A. S., Salama, K. N. and Kennedy, M. P.: An equation for generating chaos and its monolithic implementation. Int. J. Bifurcation Chaos, Vol. 12, no. 12, (2002) 2885-2896.

NOTAS EXPLICATIVAS SOBRE LAS FIGURAS

Figura 1. Amplificación de una técnica de fuente de ruido.

Figura 2. Arquitectura de doble oscilador clásico.

Figura 3. Señales de salida de reloj más rápidas y lentas.

Figura 4. Aproximación de la entropía de la secuencia $S_{dualoscillator}$ con respecto al f_{fast} / $f_{slowcenter}$ (doble oscilador con respecto al oscilador de frecuencia rápida / de centro lento).

Figura 5. Generación de números aleatorios usando la arquitectura de doble oscilador y caos de tiempo continuo.

Figura 6. Medida del oscilador modulado por caos.

Figura 7. Generación de números aleatorios usando una arquitectura de doble oscilador basada en comparador y caos de tiempo continuo.

Figura 8. Aproximación de la entropía de la secuencia S_{CDOA} con respecto a f_{fast} / $f_{slowcenter}$.

Figura 9. Generación de números aleatorios usando arquitectura de doble oscilador basado en comparador y ruido

Figura 10. Oscilador caótico autónomo MOS

Figura 11. Resultados del análisis numérico del oscilador caótico

Figura 12. Atractor caótico de la simulación del circuito post-diseño

Figura 13. Rápido y las señales de salida de reloj más lentas

Figura 14. Aproximación de la entropía de la secuencia de $S_{dualoscillator}$ con respecto a f_{fast} / $f_{slowcenter}$.

Figura 15. Resultados experimentales del oscilador caótico.

Figura 16. Medida del oscilador modulado por caos.

Figura 17. Resultados del análisis numérico del oscilador caótico.

Figura 18. Realización del circuito del atractor de doble desplazamiento.

Figura 19. Resultados experimentales del oscilador caótico.

Figura 20. Medida del oscilador modulado por caos.

Figura 21. Oscilador bipolar propuesto.

Figura 22. Resultados del análisis numérico del oscilador bipolar.

Figura 23. Oscilador CMOS propuesto.

Figura 24. Resultados del análisis numérico del oscilador CMOS.

Figura 25. Ceros de la función Melnikov calculados en la órbita homoclínica que se muestra en la esquina superior derecha.

Figura 26. Resultados experimentales del oscilador caótico bipolar.

Figura 27. Resultados experimentales del oscilador caótico CMOS.

Figura 28. Medida del oscilador modulado por caos.

REIVINDICACIONES

1. Generador de bits aleatorios que incluye una arquitectura de doble oscilador que comprende un oscilador rápido con frecuencia rápida $f_{(fast)}$ y un oscilador caótico de tiempo continuo con frecuencia de centro lento $f_{(slow\ center)}$ y un comparador para reducir la complejidad de la implementación del reloj más lento, y que se basa en la generación de bits binarios aleatorios no invertibles a partir de una de las señales del oscilador caótico, el generador de bits aleatorio que comprende:

(a) un comparador para reducir la complejidad de la implementación del reloj más lento donde, una de las señales, que corresponde a uno de los estados (x1, x2, ... o xn) del oscilador caótico de tiempo continuo se compara con un voltaje de umbral,

(b) un reloj rápido, que tiene un ciclo de trabajo del 50% que se implementa dividiendo un oscilador de baja fluctuación dentro del equipo,

(c) un flip-flop de tipo D (flip-flop D) o un flip-flop de tipo T (flip-flop T) para generar una secuencia binaria (S(CDOA)) muestreando la salida del oscilador rápido, en el aumento y/o la caída de los bordes del comparador de salida,

en donde la proporción $f_{(fast)}$ / $f_{(slow\ center)}$ es mayor que 1 y menor que 200, de modo que se obtienen números aleatorios binarios con entropía máxima.

2. Procedimiento para generar bits binarios aleatorios (S(CDOA)i) que utiliza un generador de bits aleatorio de acuerdo con la reivindicación 1 que comprende una arquitectura de doble oscilador que comprende un oscilador caótico de tiempo continuo y un comparador para reducir la complejidad de la implementación del reloj más lento y que se basa en la generación de bits binarios aleatorios no invertibles, desde uno de los estados que corresponde a una de las señale del oscilador caótico y que comprende las etapas de:

(a) determinar los tiempos de muestreo designados en la condición de transición de un estado x1, x2, ... o xn del oscilador caótico definido como x1 ... n (t) = x1 ... n (0) con dx1. ... n / dt> 0 o dx1 ... n / dt <0.

(b) generar la secuencia binaria aleatoria

i. S(CDOA)i muestreando la salida de un oscilador rápido en los tiempos de muestreo correspondientes con las transiciones de la condición de un estado definido en la etapa a; o,

ii. S(CDOA)i, por S(CDOA)i = S (CDOA) (i-1), si el bit, muestreado de la salida de un oscilador rápido en los tiempos de muestreo correspondientes a las transiciones de la condición de un estado definido en la etapa a , es 0 y S(CDOA)i = al inverso lógico de S(CDOA)(i-1), si el bit muestreado de la salida de un oscilador rápido en los tiempos de muestreo correspondientes a las transiciones de la condición de un estado definido en el paso a, es 1.

FIG - 1

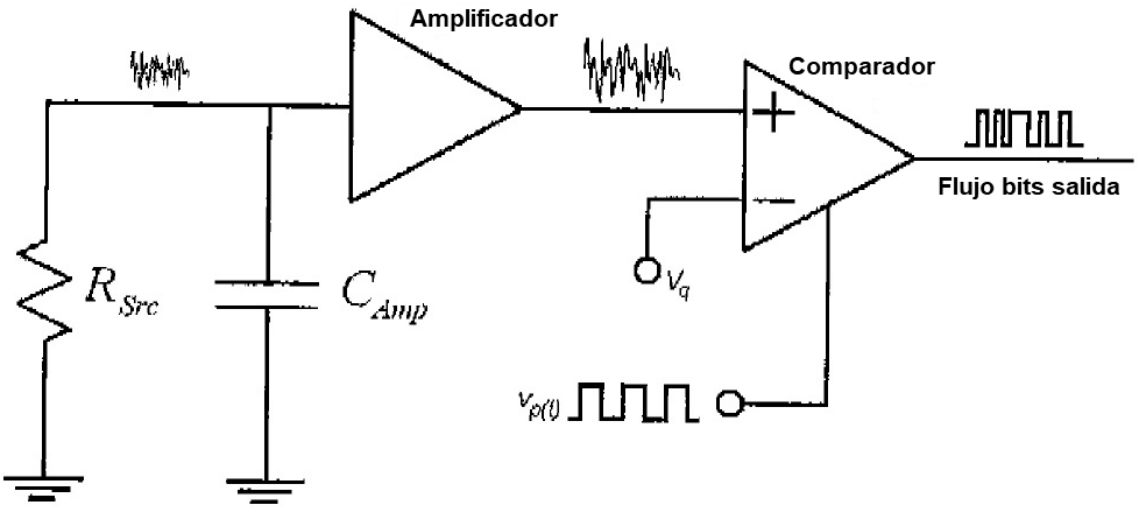
Amplificador
Comparador
Flujo bits salida
R_{Src}
C_{Amp}
V_q
$V_{p(t)}$

FIG - 2

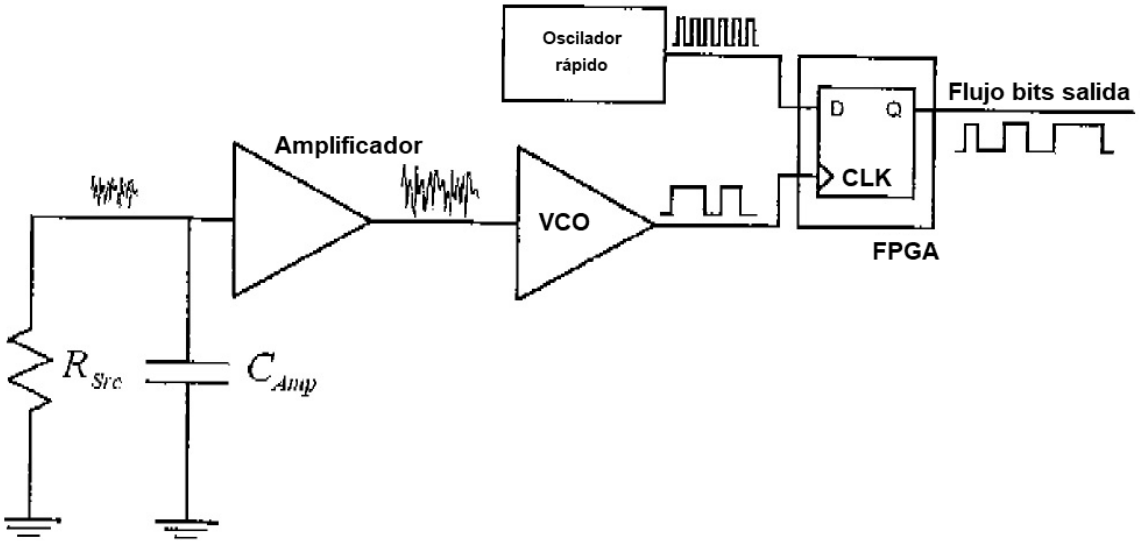
Oscilador rápido
Flujo bits salida
D
Q
CLK
Amplificador
VCO
FPGA
R_{Src}
C_{Amp}

FIG - 3

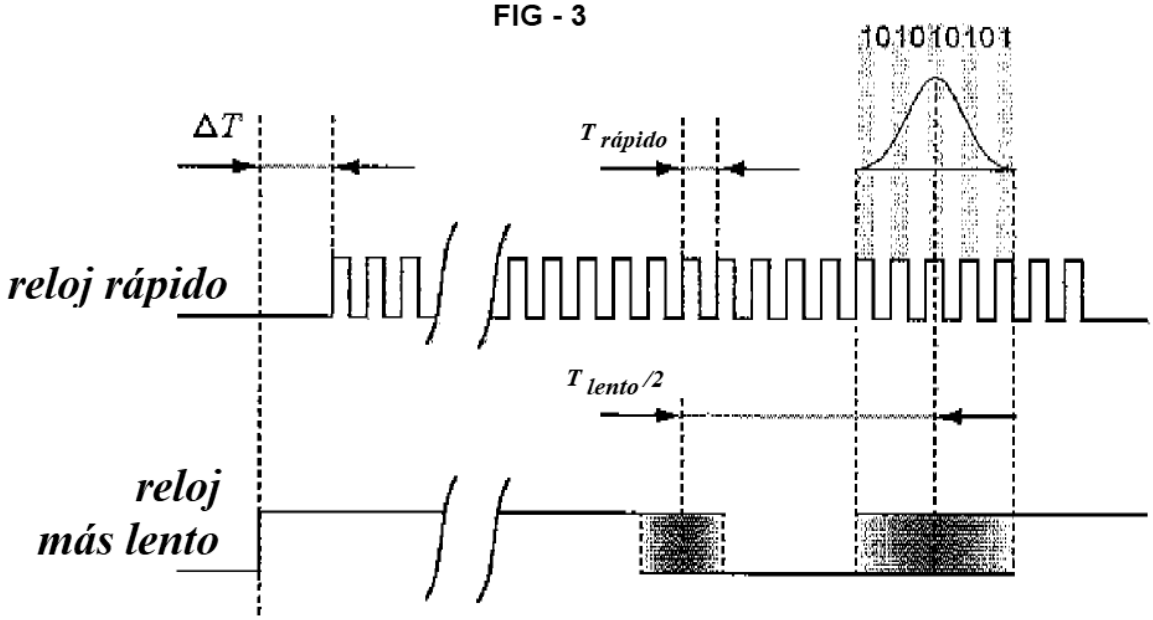
1010101010
ΔT
T rápido
reloj rápido
T lento/2
reloj
más lento

FIG - 4

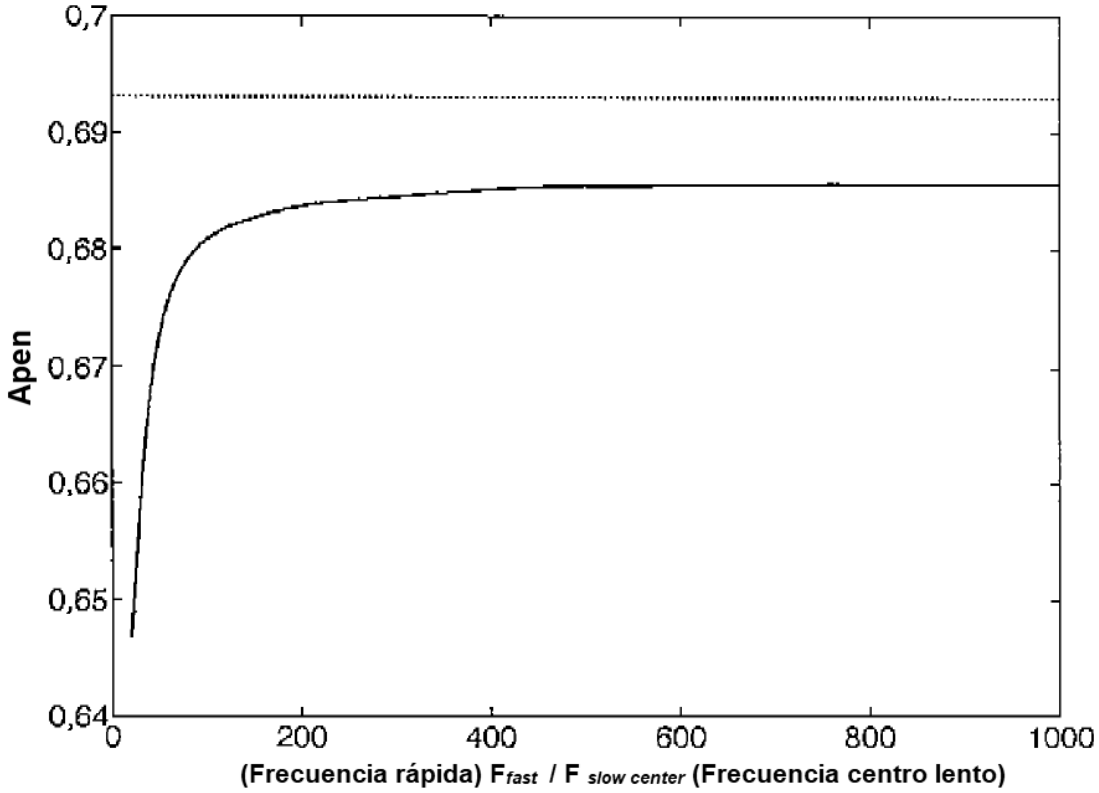
0,7
0,69
0,68
0,67
0,66
0,65
0,64
Apen
0
200
400
600
800
1000
(Frecuencia rápida) Ffast / F slow center (Frecuencia centro lento)

FIG - 5

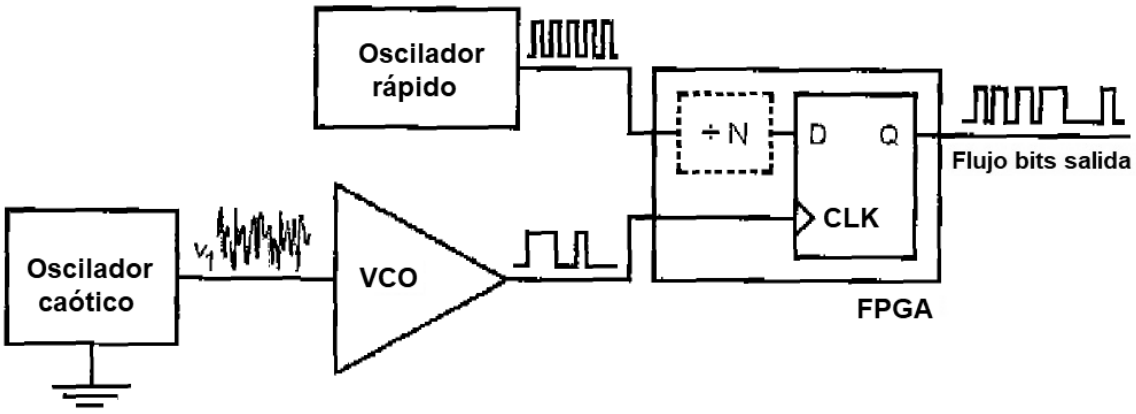
Oscilador rápido
÷N
D
Q
Flujo bits salida
CLK
Oscilador caótico
VCO
FPGA

FIG - 6

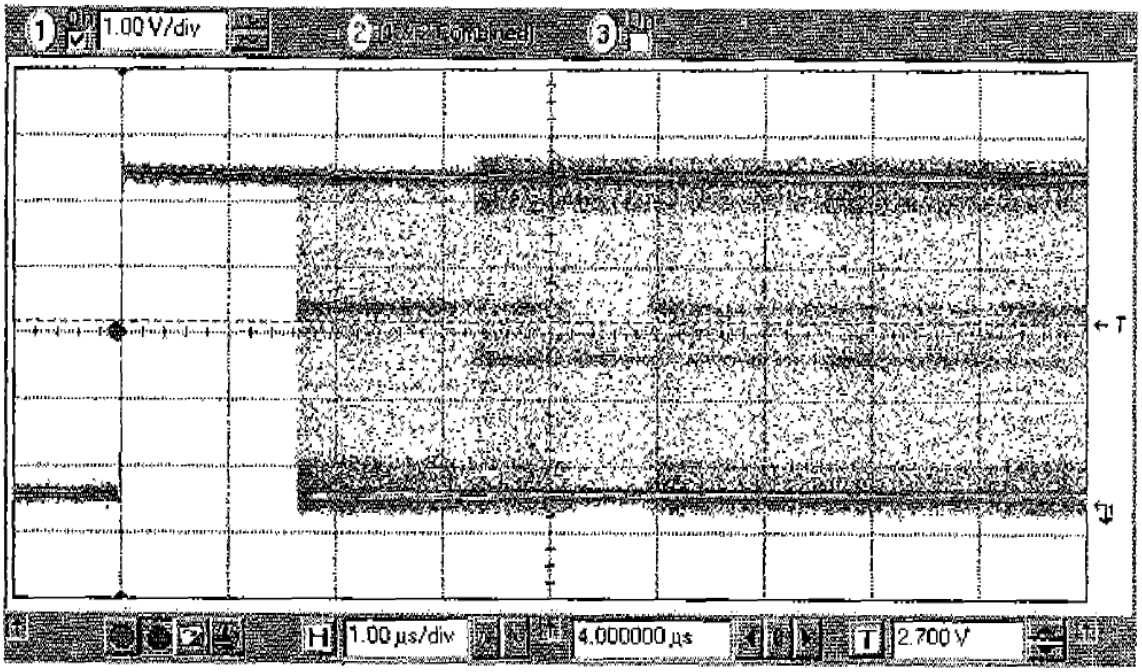
1.00 V/div
1.00 µs/div
4.000000 µs
2.700 V

FIG - 7

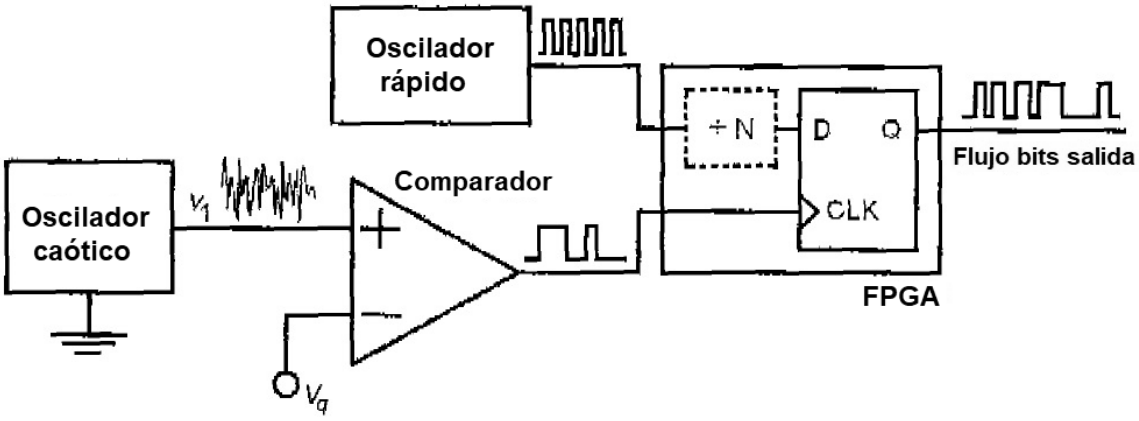
Oscilador rápido
÷N
D
Q
Flujo bits salida
Oscilador caótico
V_1
Comparador
CLK
FPGA
V_q

FIG - 8

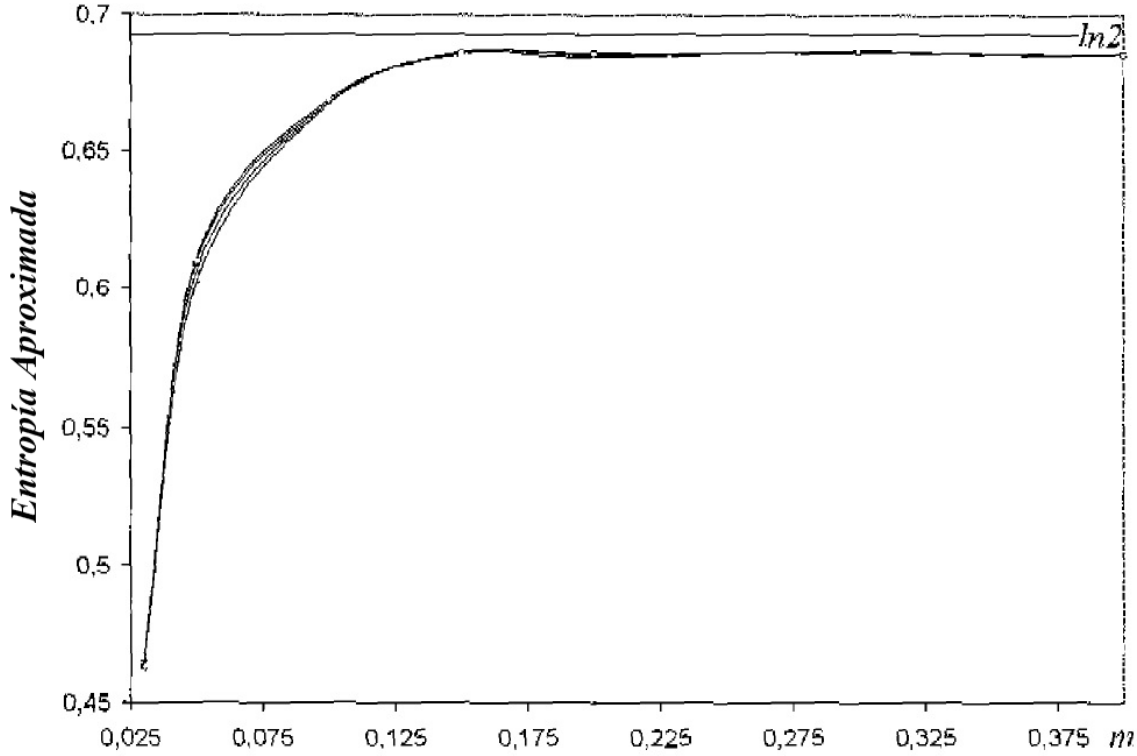
0,7
ln2
0,65
0,6
0,55
0,5
0,45
Entropía Aproximada
0,025
0,075
0,125
0,175
0,225
0,275
0,325
0,375
m

FIG - 9

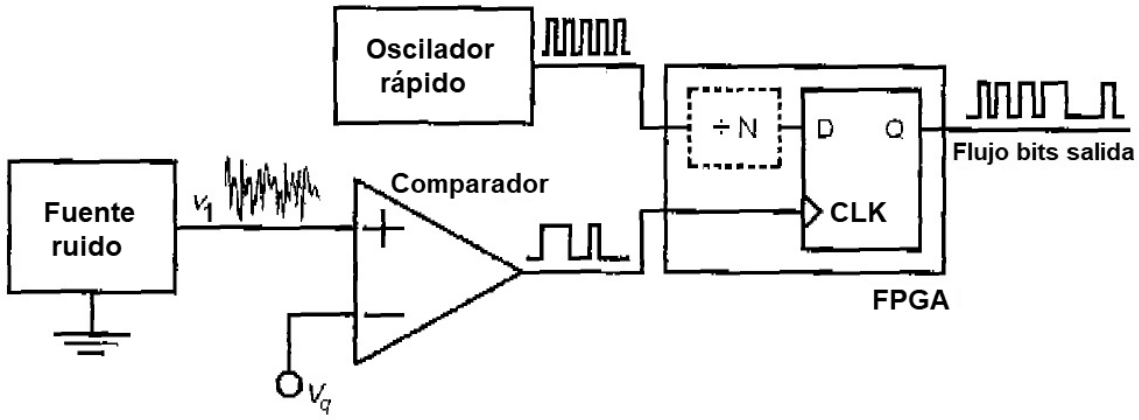
Oscilador rápido
÷N
D
Q
Flujo bits salida
Fuente ruido
V_1
Comparador
CLK
FPGA
V_q

FIG - 10

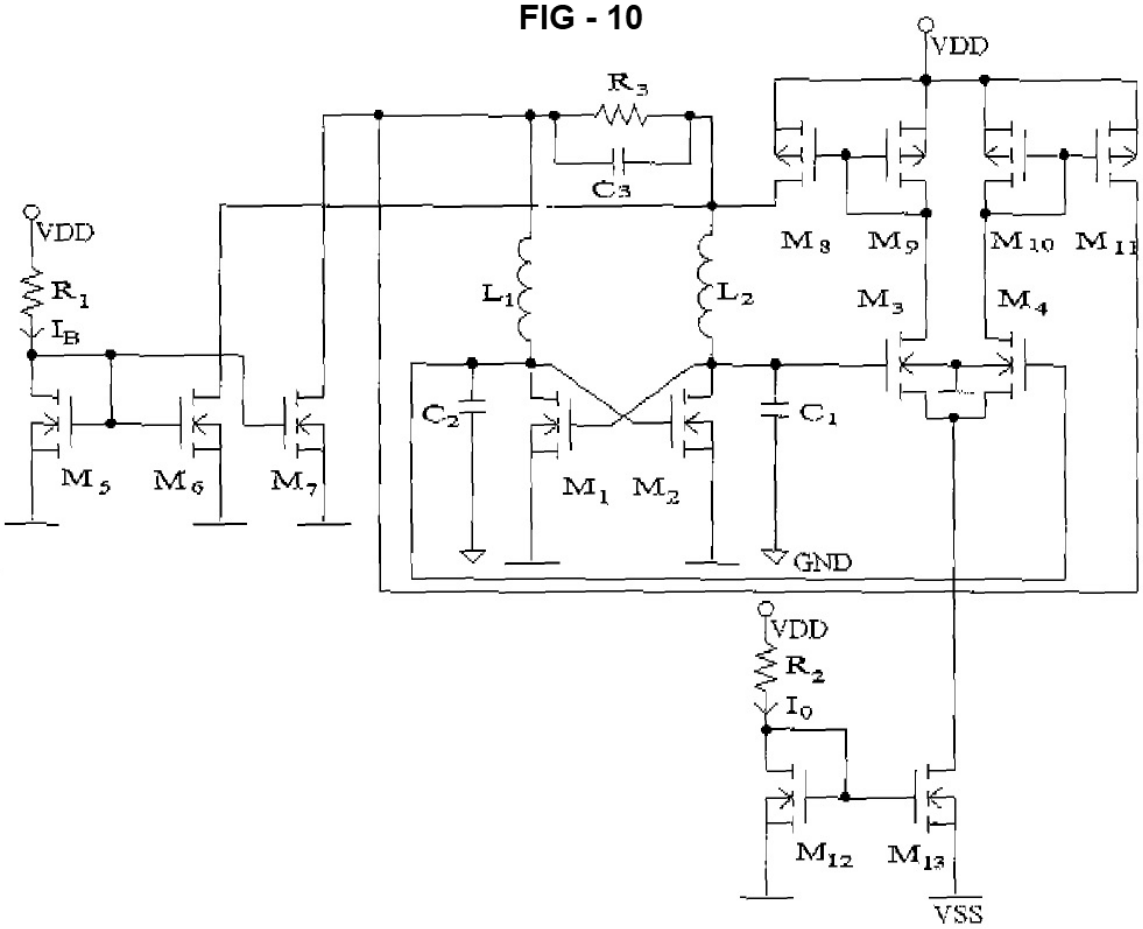
VDD
R_3
C_3
VDD
R_1
I_B
L_1
L_2
M_8
M_9
M_{10}
M_{11}
M_3
M_4
C_2
C_1
M_5
M_6
M_7
M_1
M_2
GND
VDD
R_2
I_0
M_{12}
M_{13}
VSS

FIG - 11

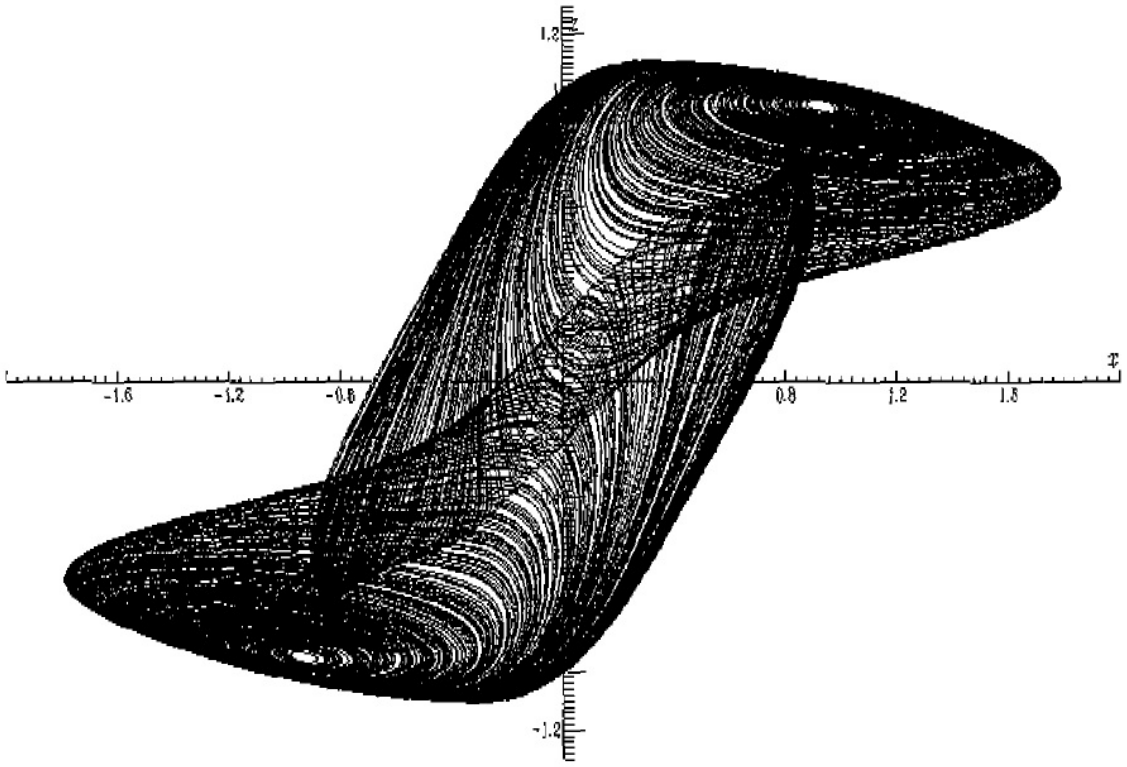
1.2
-1.6
-1.2
-0.8
0.8
1.2
1.6
x
-1.2

FIG - 12

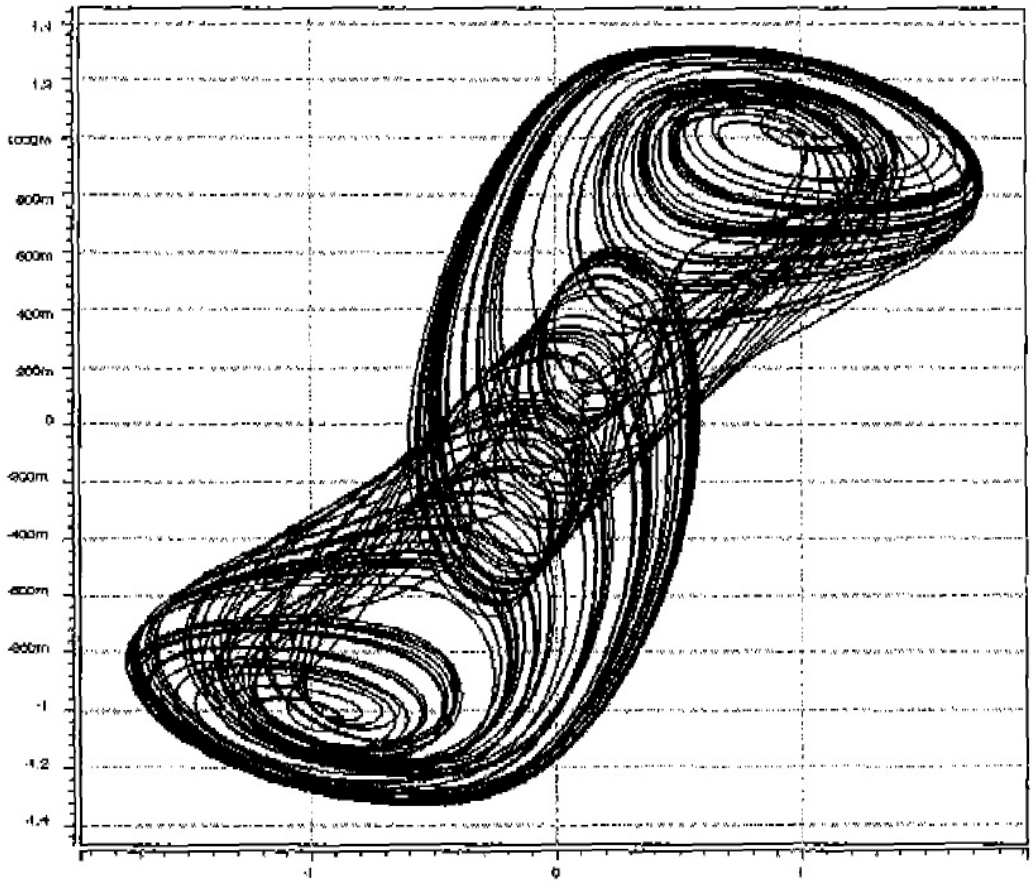
1.4
1.2
1000m
800m
600m
400m
200m
0
-200m
-400m
-600m
-800m
-1
-1.2
-1.4
-1
0
1

FIG - 13

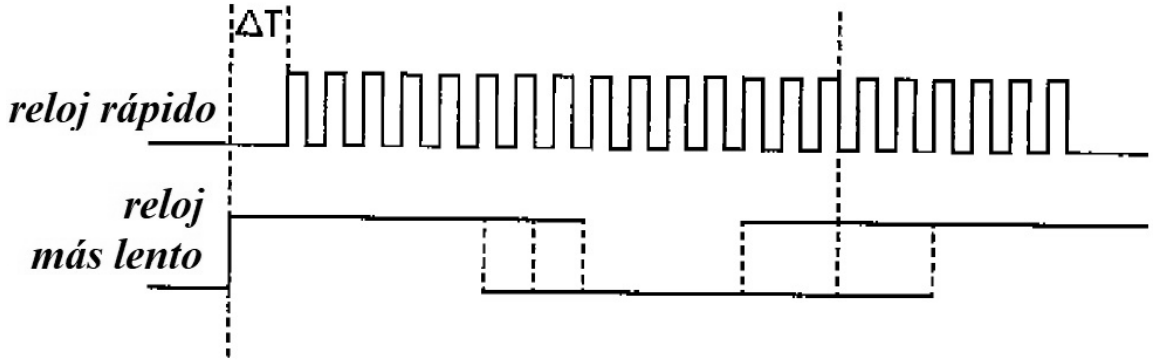
ΔT
reloj rápido
reloj
más lento

FIG - 14

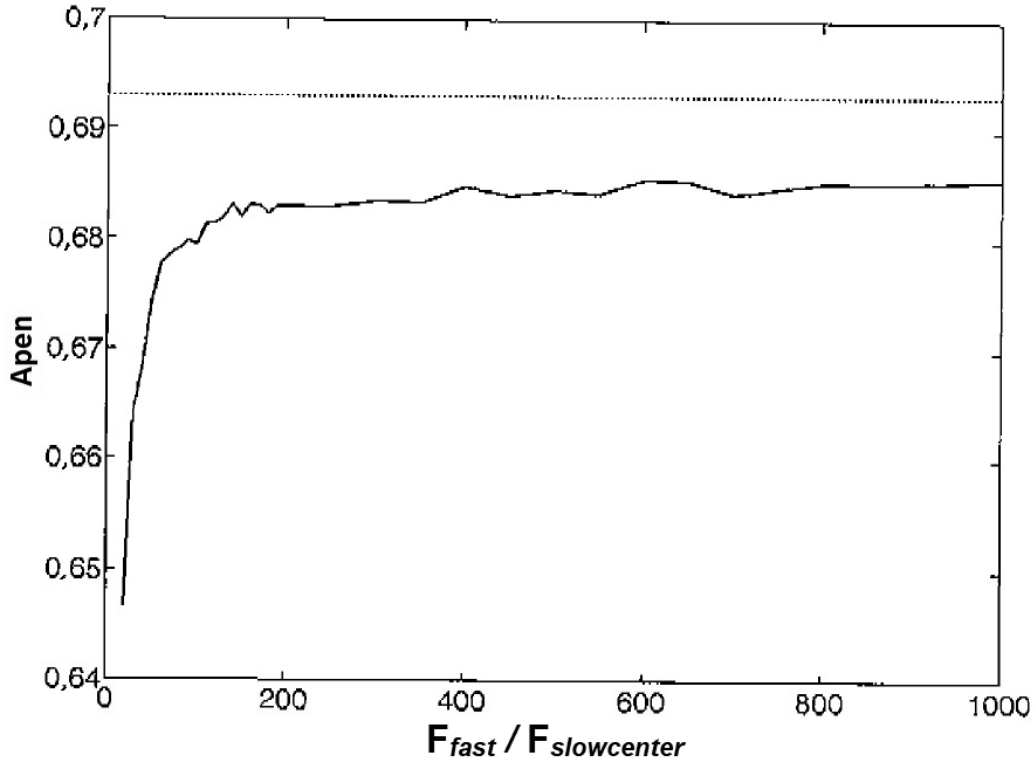
0,7
0,69
0,68
0,67
0,66
0,65
0,64
Apen
0
200
400
600
800
1000
F fast / F slowcenter

FIG - 15

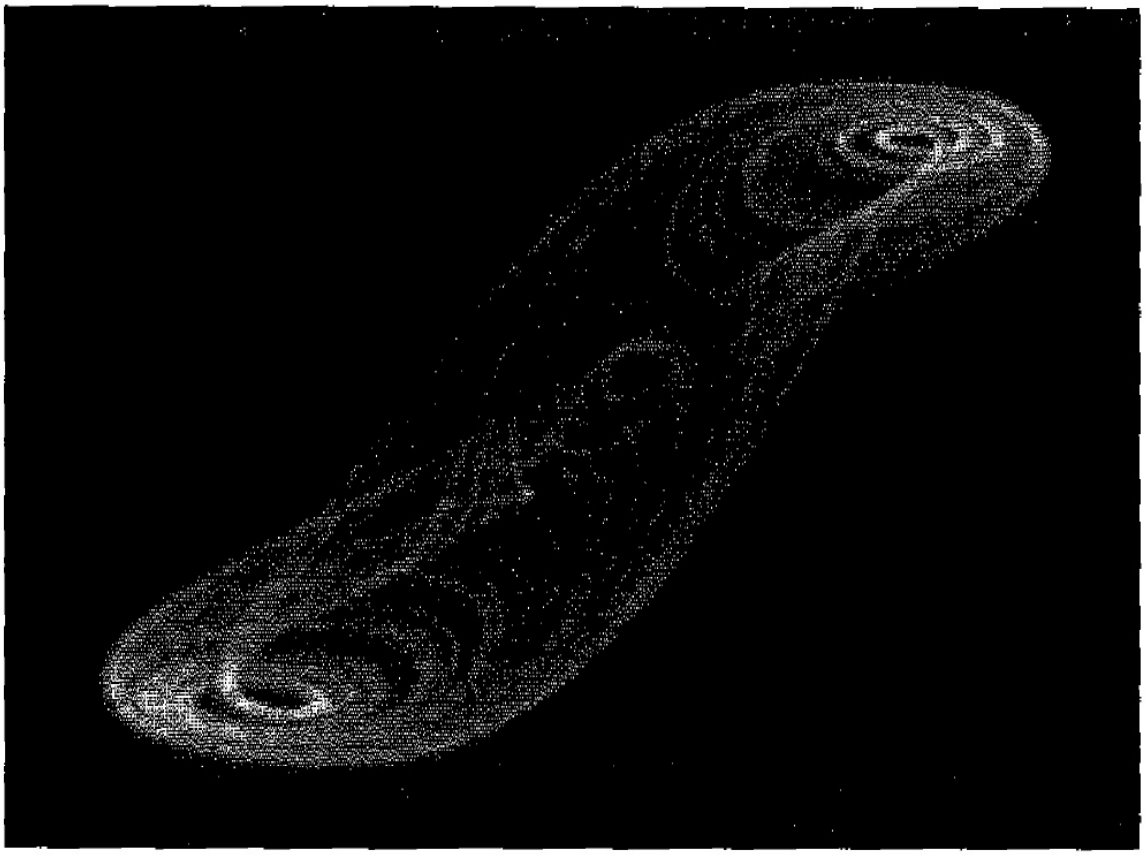

FIG - 16

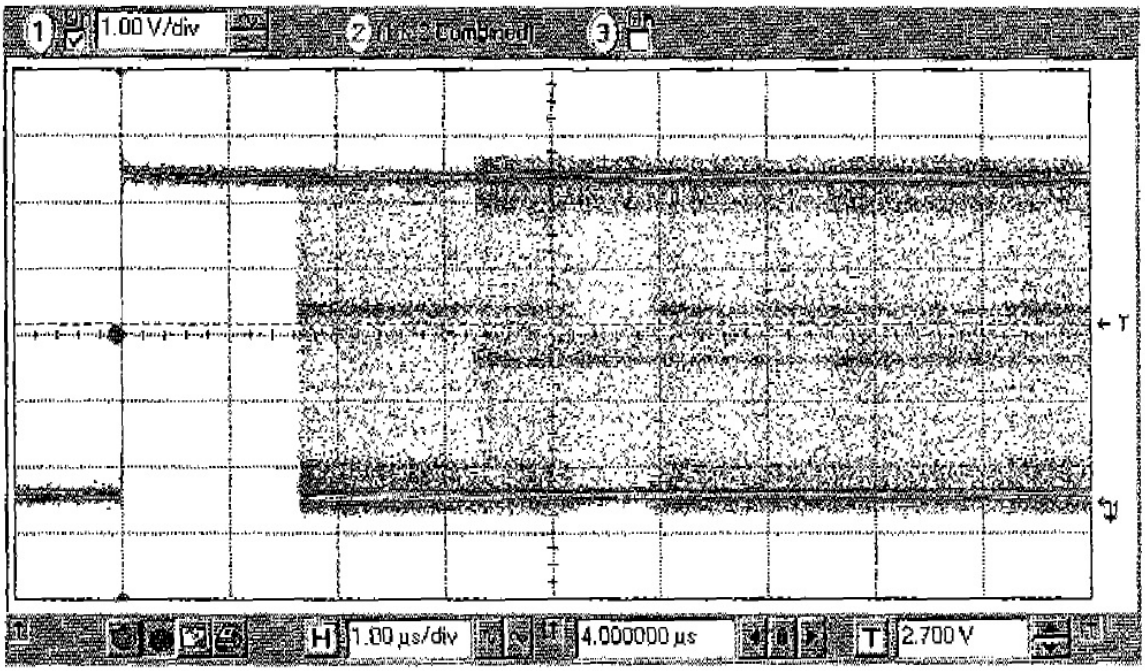

FIG - 17

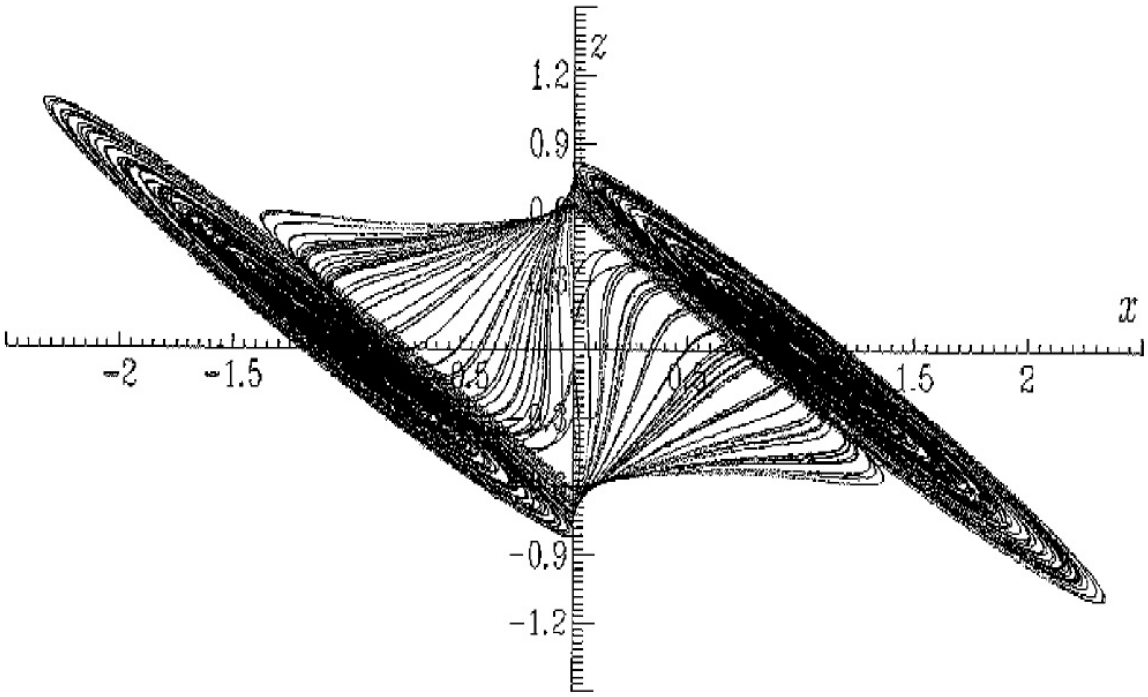
z
1.2
0.9
-0.9
-1.2
x
-2
-1.5
1.5
2

FIG - 18

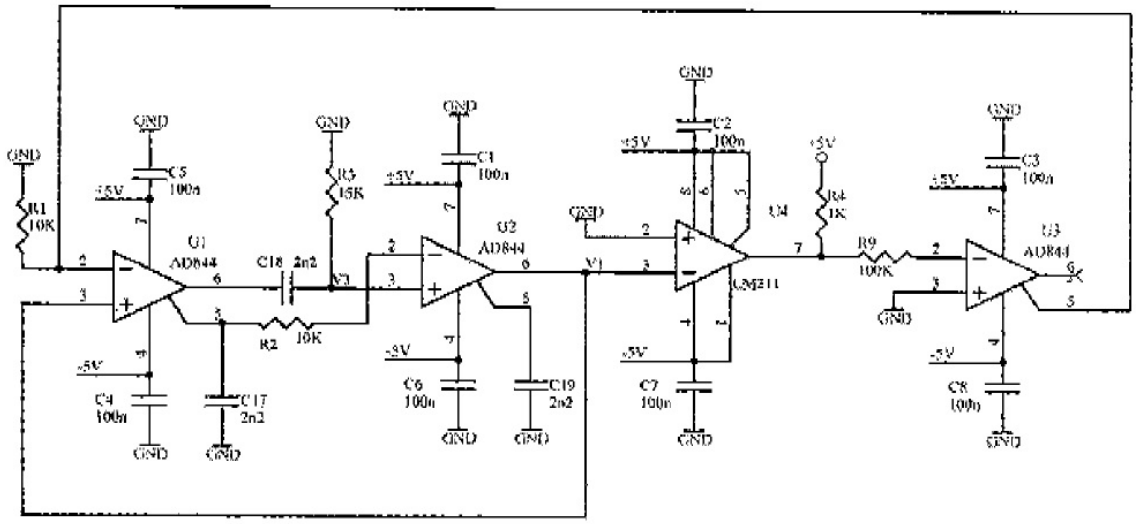
GND
+5V
-5V
U1
AD844
U2
AD844
U3
AD844
U4
OPA111
C1 100n
C2 100n
C3 100n
C4 100n
C5 100n
C6 100n
C7 100n
C8 100n
C17 2n2
C18 2n2
C19 2n2
R1 10K
R2 10K
R3 15K
R4 1K
R9 100K

FIG - 19

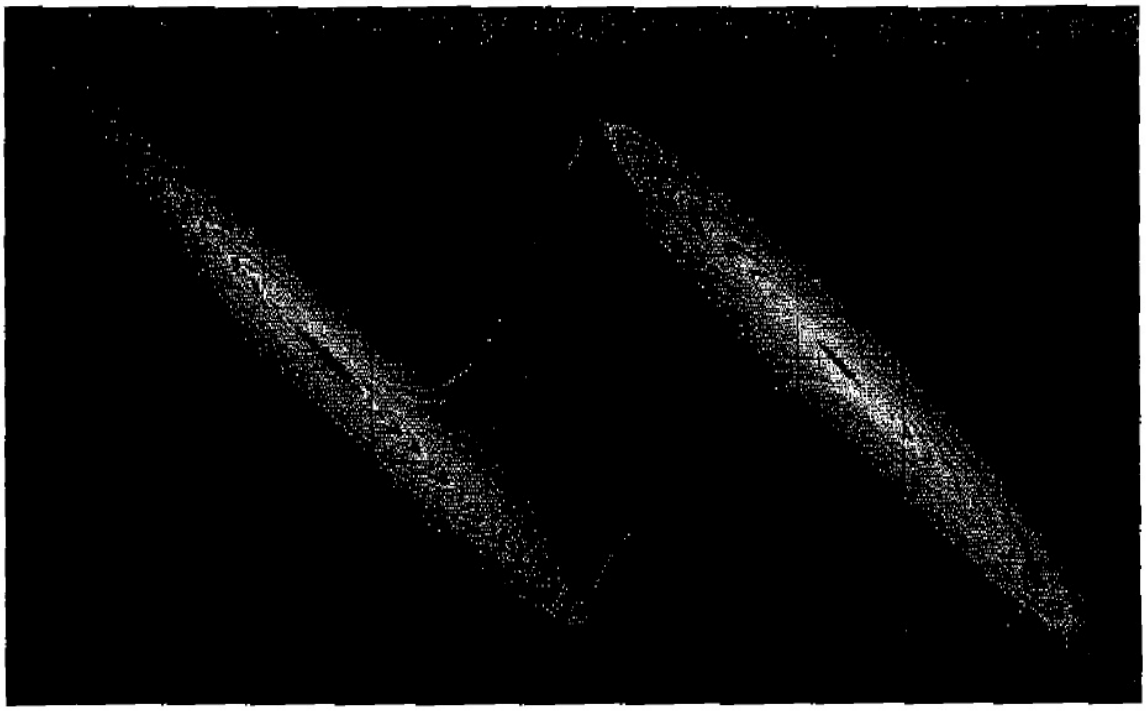

FIG - 20

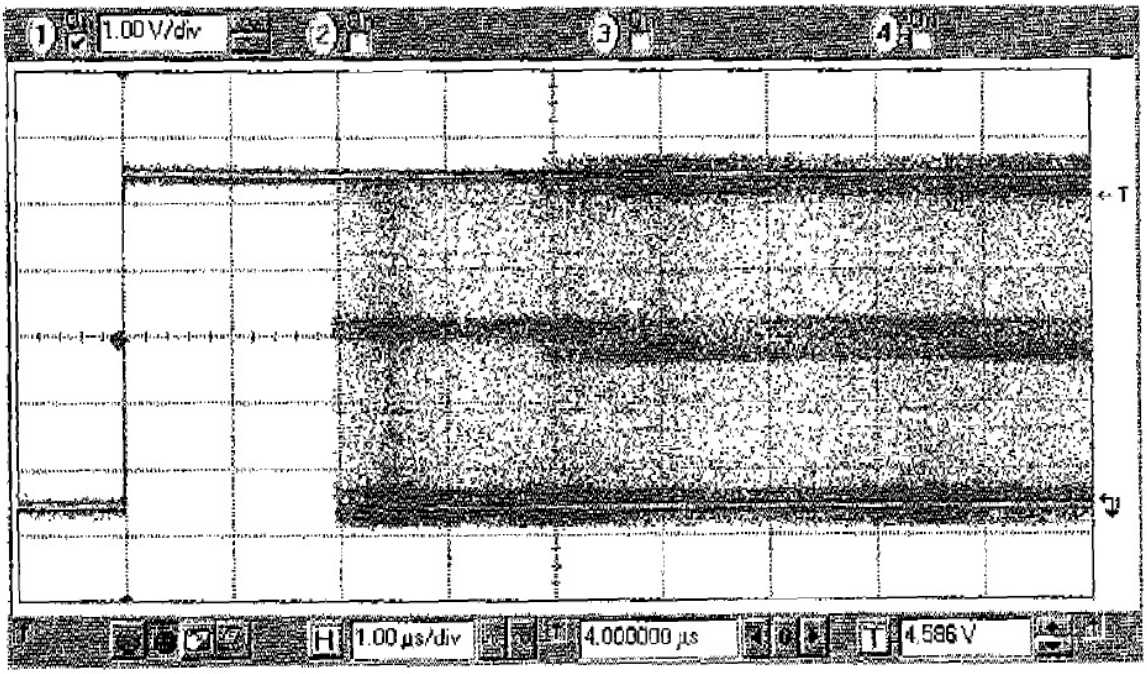

FIG - 21

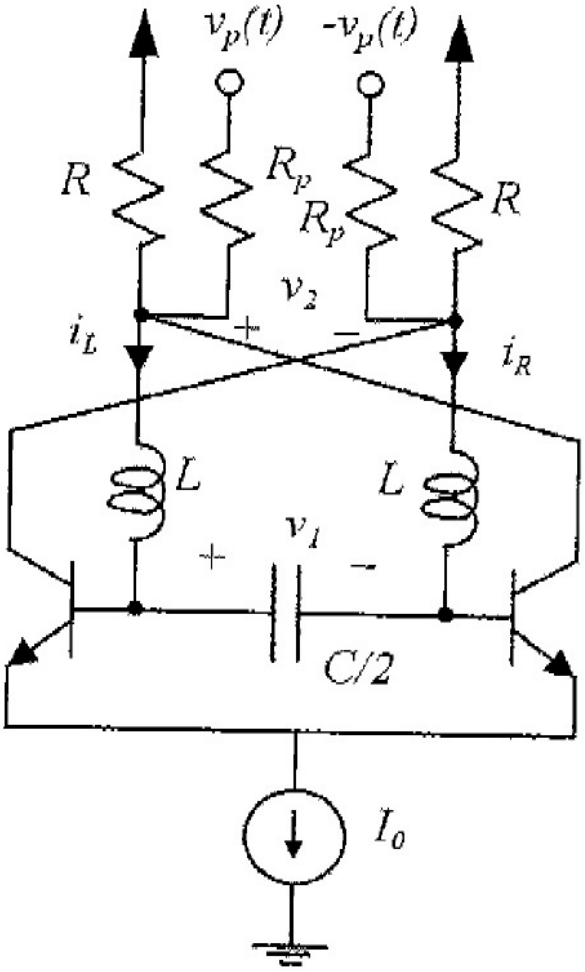

FIG - 22

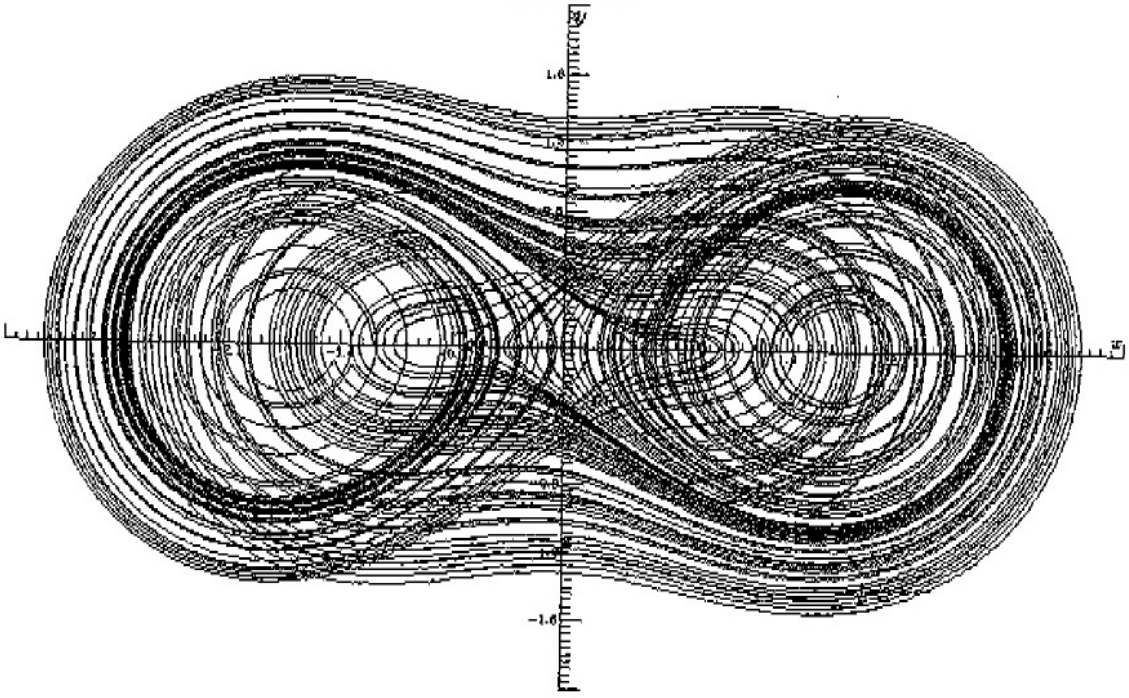

FIG - 23

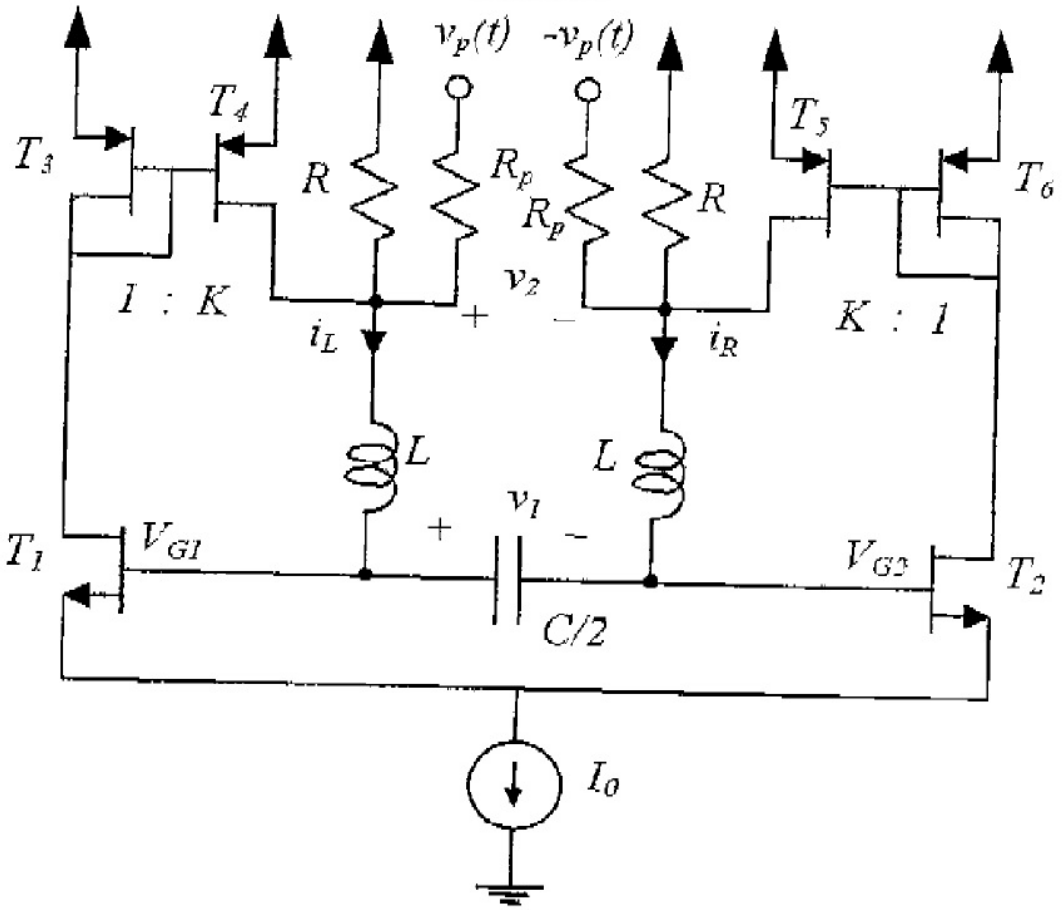
$v_p(t)$
$-v_p(t)$
T_3
T_4
T_5
T_6
R
R_p
R_p
R
v_2
I : K
K : 1
i_L
i_R
L
L
v_1
T_1
V_{G1}
V_{G2}
T_2
C/2
I_0

FIG - 24

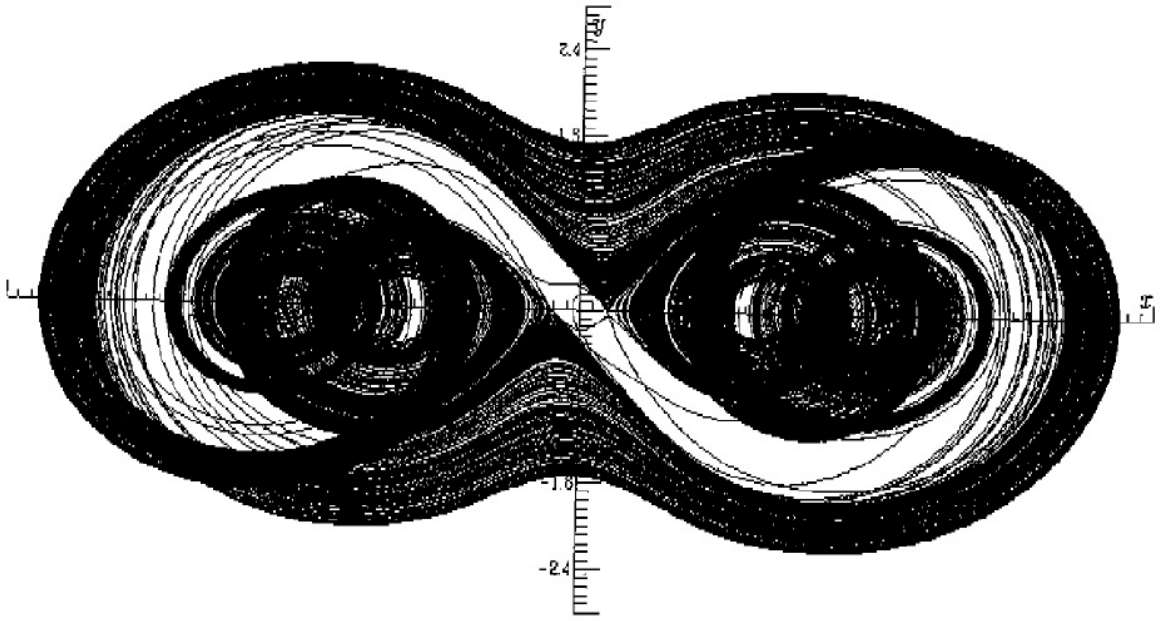
2.4
1.8
1.2
0.6
0.0
-0.6
-1.2
-1.8
-2.4

FIG - 25

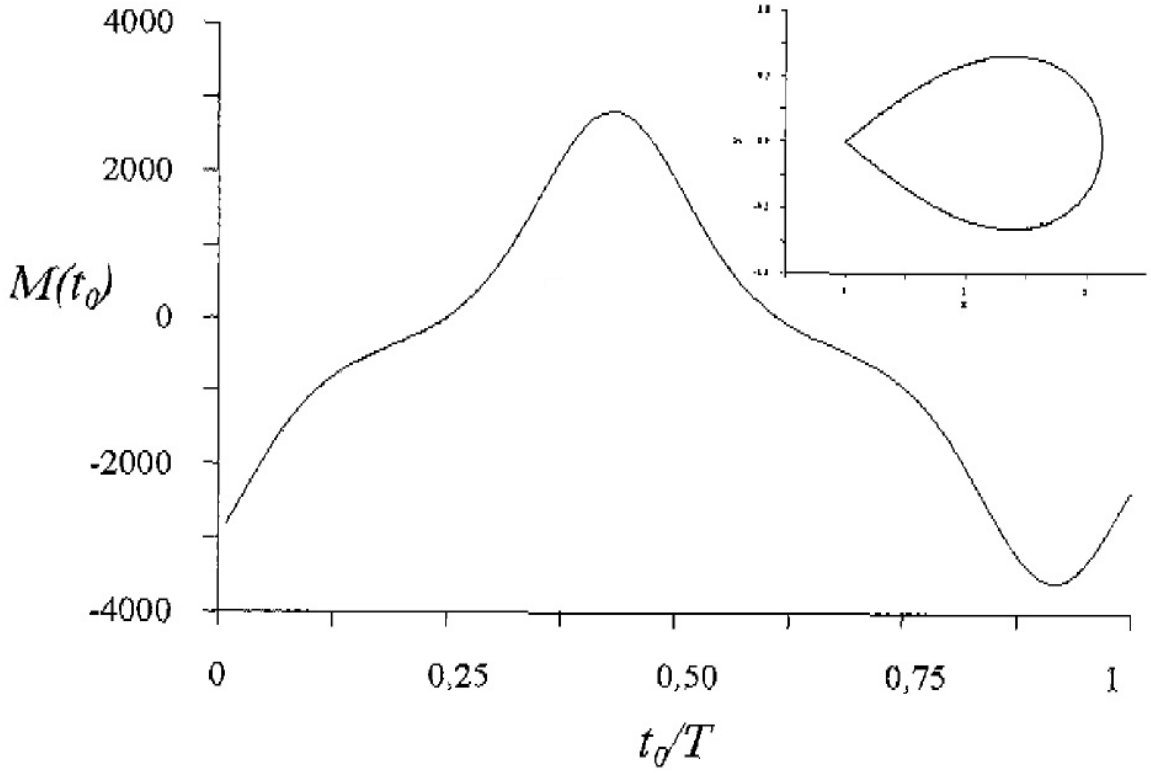

FIG - 26

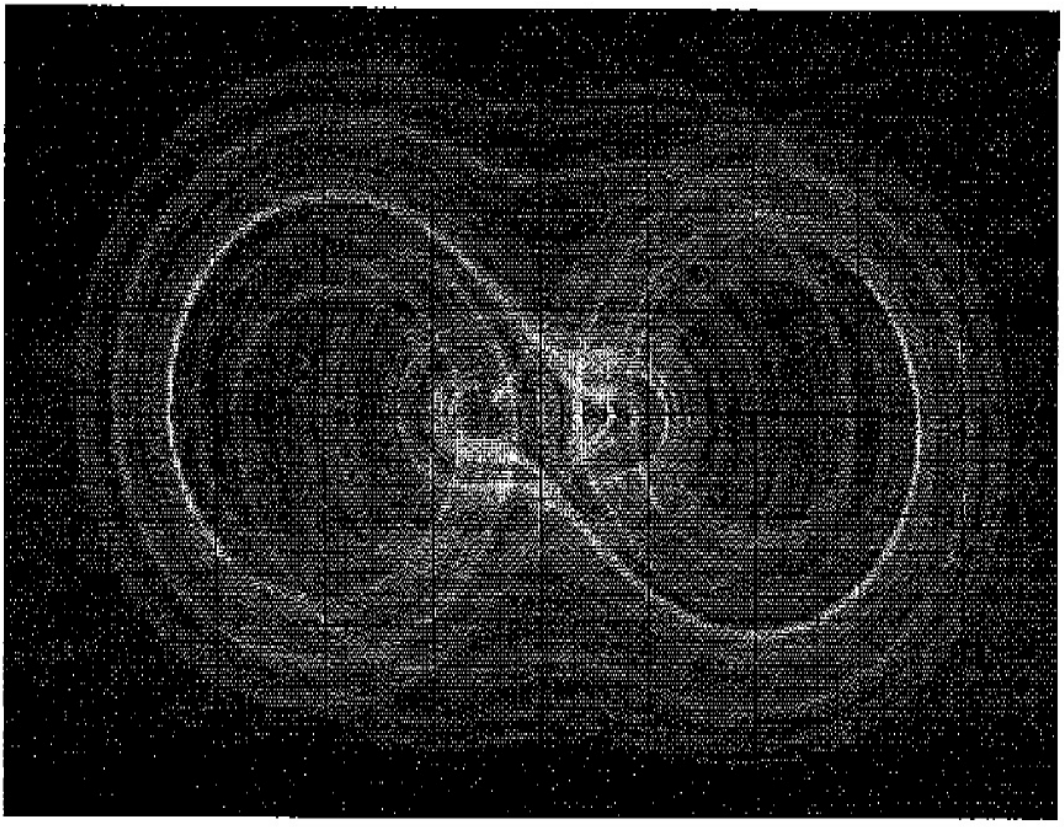

FIG - 27

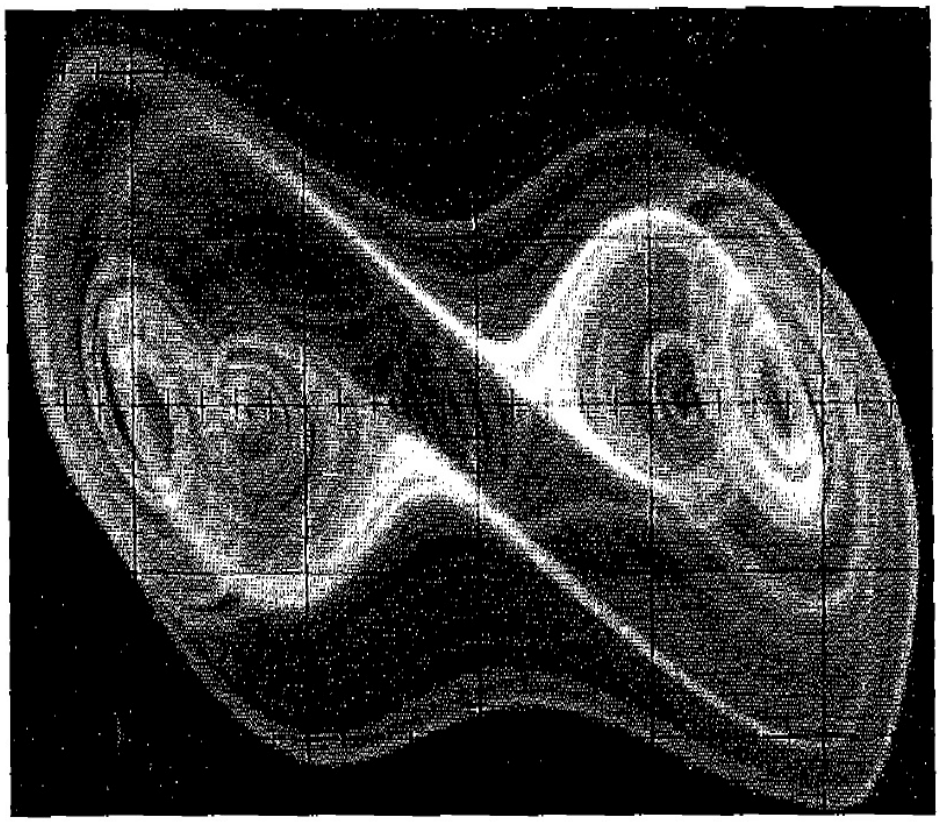

FIG - 28