# Diseño y realización hardware de un generador de números aleatorios

**Miguel Alberto Melgarejo R.**[1]

**Alexis Javier Piraján A.**[2]

## RESUMEN

Este articulo presenta la descripción, validación y caracterización de un HRNG (Hardware Random Number Generator) con salida en formato paralelo de 12 bits. Los números entregados por el generador son una representación digital del ruido térmico obtenido de un dispositivo semiconductor. Para este efecto dos dispositivos semiconductores (Bipolar simple y Bipolar zener) han sido empleados y comparados. La comparación se centra en el análisis estadístico y espectral del ruido proporcionado por cada uno de estos dispositivos. Los resultados obtenidos de este análisis indican un norte para la futura aplicación del generador diseñado.

**Palabras claves**: Generadores de números aleatorios , ruido térmico, ruido blanco gaussiano, ruido blanco uniforme, procesos estocásticos.

## ABSTRACT

This article presents the specification , validation and modeling of a HRNG (Hardware Random Number Generator) with 12 bit parallel output format. The working principle of the proposed generator consists on sampling the electrical signal obtained from the thermal noise in a semiconductor, in this sense , two semiconductors devices (BJT and bipolar Zener) have been used and compared. Statistical and spectral analyses have been employed for comparing the noise provided by these devices. Obtained results show an interesting application field for this generator.

**Keywords**: Random number generators , thermal noise , White Gaussian noise , White uniform noise , sthocastic processes

## I. INTRODUCCIÓN

La mayoría de simulaciones de montecarlo, procesos de criptografía [1] y generación de direcciones IP [2], entre otros, requieren del uso de fuentes de números aleatorios estadísticamente independientes. Hasta el momento las fuentes empleadas han sido algoritmos que generan números pseudoaleatorios (PRNGs) [3], por lo tanto la condición de independencia estadística en algunos casos no se logra, haciendo que las aplicaciones fallen [4]. Es de especial importancia el caso de las aplicaciones de seguridad en la transmisión de información [1].

Teniendo en cuenta este problema, se hace necesario buscar nuevos métodos para la generación de números aleatorios. Una tendencia es capturar la dinámica de un proceso estocástico real, ejemplo de ello es el ruido atmosférico, el sonido de la lluvia al caer , el decaimiento de un material radioactivo [5] o el ruido térmico en semiconductores [6].

De los ejemplos mencionados anteriormente, es claro que desde un punto de vista práctico, el uso de semiconductores como fuentes de ruido , es una estrategia adecuada de fácil realización. En la actualidad se ha aprovechado este fenómeno en el desarrollo de generadores seriales de cadenas de bits aleatorias (HRNGs) [7].

El trabajo descrito en este documento se centran en el diseño, construcción y modelado de un generador hardware de números aleatorios partiendo del ruido térmico en un semiconductor, con la particularidad que estos números son entregados en un formato paralelo de 12 bits.

Para llevar a cabo este desarrollo se empleó la siguiente metodología: en primer lugar se escogieron dos junturas semiconductoras (bipolar simple y bipolar zener), luego una arquitectura para amplificar y digitalizar la señal de ruido proveniente de cada una de estas junturas. Por último, las señales de ruido fueron caracterizadas de forma estadística[8] y espectral [9], con el fin de modelar los procesos estocásticos correspondientes[10].

De acuerdo a los resultados obtenidos de la caracterización de las junturas, el sistema planteado tiene propiedades adecuadas para ser llevado al contexto de algunas de las aplicaciones mencionadas al comienzo.

## II. ARQUITECTURA DEL HRNG.

Un generador hardware convencional de cadenas de bits aleatorias se encuentra formado por tres etapas[7], tal como se muestra en Fig. 1. La etapa de generación de ruido es un dispositivo semiconductor polarizado inversamente, por lo tanto, la única actividad electrónica en el dispositivo será aquella debida a las corrientes de fuga térmica. Los niveles de tensión asociados a dicha actividad electrónica aleatoria se encuentran en el orden de microvolts[6], esto hace que sea necesaria una etapa de amplificación que lleve las variaciones de voltaje en la juntura ha-

[1] Miembro Grupo de Investigación LAMIC Laboratorio de Automática, Microelectrónica e Inteligencia Computacional, Universidad Distrital Francisco José de Caldas.

Artículo recibido en Septiembre 10 de 2002
Aceptado el 13 de Noviembre 2002

La propuesta presentada en este trabajo emplea un conversor AD de 12 bits en lugar de un cuantificador de un solo bit, se busca de esta forma mejorar la representación digital del ruido proveniente de la juntura.

cia niveles adecuados para su posterior tratamiento y digitalización. Los amplificadores involucrados en esta etapa deben poseer una relación señal a ruido elevada de manera que no amplifiquen su propio ruido térmico.

La ultima etapa se encarga de la digitalización de la actividad electrónica, luego se deben considerar dos aspectos importantes : cuantificación y frecuencia de muestreo. Una revisión de estado de arte indica que la mayoría de HRNGs emplean tan solo dos niveles de cuantificación , es decir , que su salida será una secuencia de unos y ceros que el sistema receptor se encargará de almacenar y dar un formato paralelo.

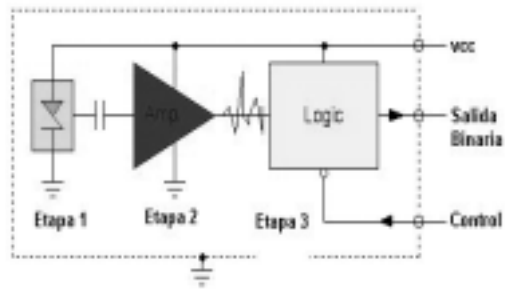


Fig.1. Arquitectura de un HRNG convencional.

La secuencia aleatoria binaria es generada por un sistema comparador. Este sistema se encarga de observar el ruido (amplificado) proveniente de la juntura y compararlo con un umbral , cuando el ruido supera este valor la salida del comparador será un uno en caso contrario se tendrá un cero. Dado que este comparador es un dispositivo electrónico tendrá un tiempo de respuesta ante los cambios de la señal de ruido, este aspecto limita su operación en cuanto a velocidad se refiere. Esto sugiere que la salida del comparador no podrá ser capturada a cualquier frecuencia de muestreo, de hecho, esta deberá ser menor que la impuesta por el retardo de respuesta del sistema comparador.

La propuesta que se presenta en este trabajo conserva las dos etapas iniciales de un HRNG convencional , y entra a modificar la etapa de digitalización. El sistema comparador es reemplazado por un conversor analógico digital de 12 bits, luego a la salida de este conversor se obtendrá una representación de la señal de ruido proveniente de la juntura sobre una base de 212 posibles valores. En fig. 2 se puede apreciar la diferencia entre un HRNG convencional y el sistema propuesto, en cuanto al formato de salida se refiere.

El sistema de conversión analógico digital empleado es una tarjeta de adquisición de datos PCI6024E de la firma National Instruments , la cual fue acoplada a la salida del sistema de amplificación. Se emplearon las herramientas de programación gráfica de Labview 6.0 para capturar y organizar los valores muestreados. Los números capturados se organizaron en una matriz tal como se presenta en fig.3 . Cada una de las filas de la matriz es una realización del proceso estocástico bajo observación, por lo tanto las columnas representan los valores puntuales de estas realizaciones en un tiempo to, es decir, variables aleatorias.

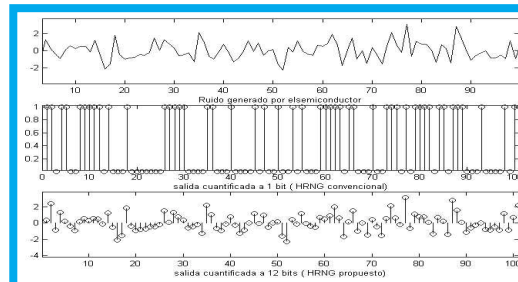


Fig 2. Comparación entre HRNGs convencional y propuesto.

| | | | |
|---|---|---|---|
| $X_o(0)$ | $X_0(1)$ | ..... | $X_0(m)$ |
| $X_1(0)$ | $X_1(1)$ | ..... | $X_1(m)$ |
| | | | |
| $X_n0)$ | $X_n(1)$ | ..... | $X_n(m)$ |

Fig 3. Organización de los números, n realizaciones de longitud m.

## III. CARACTERIZACIÓN DE LAS FUENTES DE RUIDO TÉRMICO.

Como fuentes de ruido térmico se emplearon dos junturas PN, la primera de ellas, una bipolar de un transistor BJT, y la segunda, una juntura bipolar tipo ZENER. Con el fin de obtener el modelo de ruido de cada una de estas junturas, se llevaron a cabo pruebas estadísticas, de autocorrelación y densidad espectral de potencia.

### 3.1.Pruebas estadísticas

Previo a la prueba estadística, dos bases de datos fueron creadas para almacenar las realizaciones de los ruido obtenidos de las junturas. La estructura de estas bases de datos sigue la organización presentada en fig 3, con un total de 600 realizaciones en promedio, cada una de estas con una longitud de 1000 datos. Estas bases de datos fueron construidas como arreglos de LABVIEW®, y luego transportadas a hojas de cálculo en EXCEL®. Se empleo CRISTAL BALL®, un paquete de análisis estadístico para llevar a cabo las pruebas de ajuste a ciertas distribuciones.

Las pruebas de ajuste se ejecutaron sobre las filas de las matrices, dado que corresponden a variables aleatorias en tiempos particulares del proceso. Con el fin de determinar la característica de estacionaridad del proceso, se tomaron filas a intervalos de tiempo iguales.

Las pruebas de ajuste revelaron que tanto el ruido proveniente de la juntura BJT como el proveniente de la juntura ZENER son estacionarios; el primero tiene distribución gaussiana y el segundo distribución uniforme.

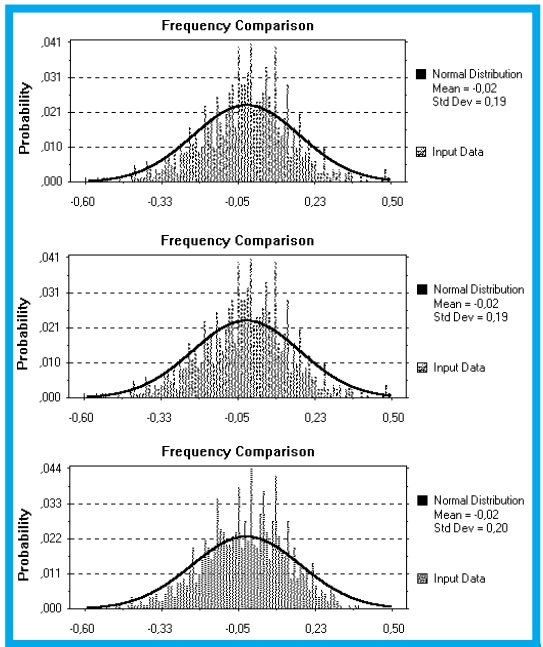


**Fig 4. Ajustes representativos para las variables aleatorias del**

Tabla 1. Resultados de las pruebas de ajuste, juntura BJT.

| Tiempo | Distribución | Media | Std_dev | Chi | Ks | Ad |
|---|---|---|---|---|---|---|
| 200ms | N | -0.02 | 0.2 | 88.16 | 0.0687 | 8.4217 |
| 400ms | N | -0.03 | 0.19 | 64.92 | 0.0699 | 7.5855 |
| 600ms | N | -0.02 | 0.18 | 56.45 | 0.0506 | 4.1892 |
| 800ms | N | -0.03 | 0.17 | 60.37 | 0.05 | 4.4 |
| 1000ms | N | -0.02 | 0.19 | 66.32 | 0.0634 | 6.8037 |

**N**: Disribución normal. **Chi**: Prueba de chi cuadrado.
**Ks**: Prueba de Kolmogorov-Smirnov. **Ad**: Anderson Darling.

En primer lugar se exponen los resultados de la caracterización estadística de la juntura bipolar BJT. Estos resultados se resumen en fig 4, donde se presentan algunas de las distribuciones obtenidas, las cuales reflejan el comportamiento de una serie de 30 ajustes realizados. En la tabla 1 se presentan las estadísticas de primer y segundo orden al igual que los índices de varias pruebas de ajuste. El criterio de decisión para determinar la naturaleza de las variables aleatorias, fue la comparación de los resultados presentados en la tabla 1, y los obtenidos para otras distribuciones. De hecho la herramienta de análisis, ajusta los datos y presenta la distribución normal como la mejor aproximación. Es importante observar que las estadísticas presentadas en la tabla 1, tienden a conservarse, presentando pequeñas fluctuaciones a través del tiempo. Este comportamiento fue observado para las múltiples pruebas que se realizaron, indicando en primera medida que el ruido proveniente de la juntura bipolar es estacionario, y en cada tiempo corresponde a una variable aleatoria con distribución gaussiana.

Tabla 2. Resultados de las pruebas de ajuste para la juntura zener.

| Tiempo | Distribución | Prob. | Min.-Max | Chi | Ks | Ad |
|---|---|---|---|---|---|---|
| 200ms | U | 0.076 | 0.09-0.18 | 66.3125 | 0.1579 | 7.1726 |
| 400ms | U | 0.074 | 0.08-0.18 | 31.43 | 0.1020 | 4.2054 |
| 600ms | U | 0.072 | 0.04-0.14 | 31.01 | 0.1148 | 5.7181 |
| 800ms | U | 0.074 | 0.06-0.16 | 79.53 | 0.1398 | 6.6340 |
| 1000ms | U | 0.073 | 0.03-0.13 | 31.85 | 0.0926 | 3.5514 |

**U**: Disribución uniforme. **Chi**: Prueba de chi cuadrado.
**Ks**: Prueba de Kolmogorov-Smirnov. **Ad**: Anderson Darling.

Para la juntura tipo zener se empleó la misma metodología de análisis expuesta anteriormente, y los resultados se resumen en Fig 5 y tabla 2.

Las pruebas de ajuste, mostraron de forma clara que el intervalo entre el mínimo y máximo de los datos siempre tiene la misma longitud y la diferencia en la probabilidad entre intervalos es mínima. A su vez, las pruebas de ajuste, mostraron que la distribución que mejor se ajusta a los datos obtenidos es la uniforme.

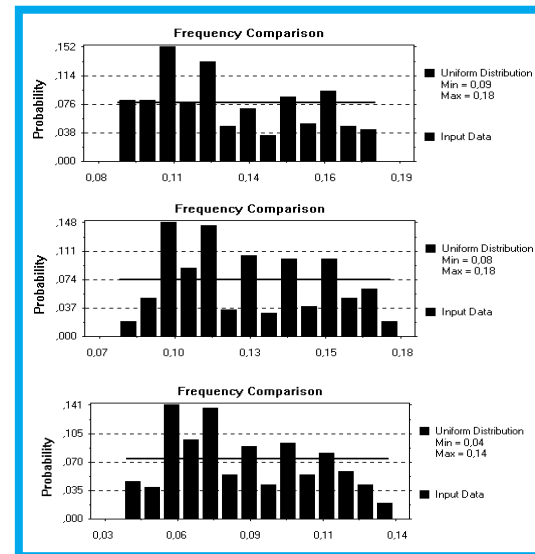


**Fig. 5. Ajustes representativos para las variables aleatorias del ruido ZENER.**

El ruido generado a partir de la juntura ZENER, mostró propiedades de estacionaridad, en donde para varios tiempos del proceso las estadísticas son similares, Fig. 5.

## 3.2. Pruebas de autocorrelación

Para llevar a cabo estas pruebas se exportaron algunas de las columnas de la matriz, (realizaciones del proceso), hacia MATLAB, donde se obtuvo su autocorrelación. En cuanto a la realización, no se tuvo ningún criterio de selección, dado que la intensión en este caso es identificar la independencia estadística de los números. En Fig 6 se presentan tres pruebas de autocorrelación, para el ruido proveniente de la juntura BJT.

De acuerdo a Fig. 6. se observa que la autocorrelación es dominada por un impulso en t=0, frente a una componente de baja amplitud que se distribuye sobre el intervalo de 2 segundos. Este mismo comportamiento se observo en las múltiples pruebas realizadas, esto hace suponer que el ruido es de naturaleza blanca. Es importante notar que el valor del impulso observado en diferentes pruebas tiene un valor aproximado de 0.04. Este hecho valida los resultados obtenidos en la tabla 1, donde se presenta una desviación estándar promedio de las variables aleatorias de 0.2.

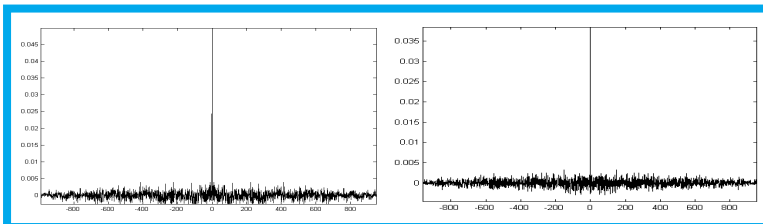

Fig 6. Autocorrelación del ruido BJT.

Fig. 7, presenta los resultados de autocorrelación del ruido generado por la juntura ZENER, al igual que para el BJT, las gráficas anteriores muestran un pico dominante para t=0, y para el resto del tiempo existe una pequeña componente, lo cual hace que el ruido tenga una naturaleza blanca, además el pico de la gráfica corresponde al valor medio de la densidad espectral de potencia como se puede apreciar en el siguiente apartado.

La densidad espectral de potencia del ruido proveniente de ambas junturas tiende a ser uniforme sobre toda la ventana de muestreo, en ese sentido la propiedad de independencia estadística puede ser garantizada.

### 3.3. Análisis espectral

Se tomaron las transformadas de Fourier de varias autocorrelaciones para luego ser promediadas (Periodograma) [10], con el fin de concluir acerca de la densidad espectral de potencia del ruido y determinar su grado de pureza [7].

En Fig.8 se presenta la densidad espectral de potencia del ruido BJT. Se observa que su valor promedio corresponde al promedio de los valores pico de las autocorrelaciones, esto demuestra que la energía del ruido tiende a distribuirse uniformemente sobre todo el espectro.

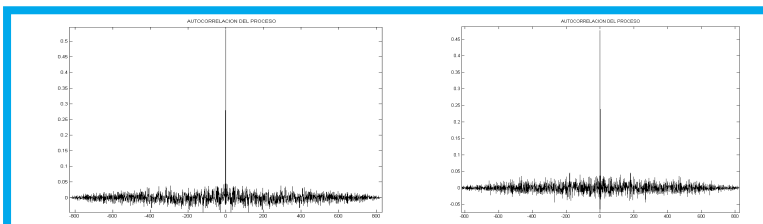

Fig 7. Autocorrelación del ruido ZENER.

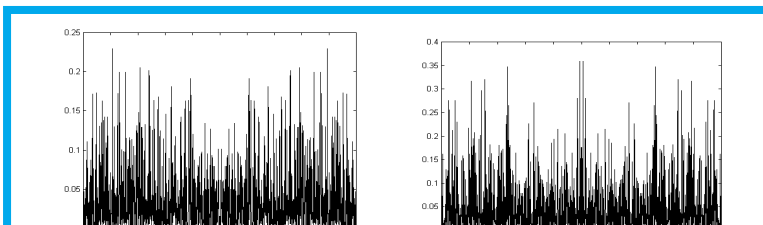

Fig. 8. Densidad espectral del ruido generado a partir de la juntura BJT.

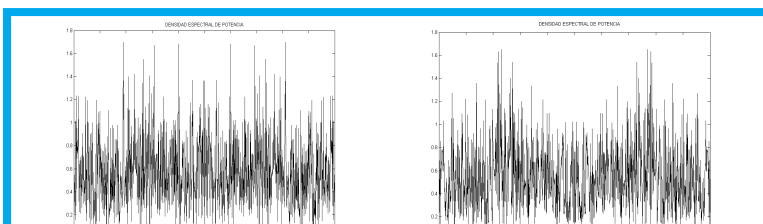

Fig 9. Densidad espectral de potencia del ruido generado por la juntura ZENER.

El análisis espectral de la autocorrelación es útil también para observar la posible presencia de señales contaminantes tal como armónicos de línea. Es claro que la presencia de estas señales determinísticas introducen cierta regularidad en las cadenas de números generadas, lo cual disminuye la independencia estadística de las mismas.

## IV. CONCLUSIONES

Se ha presentado una propuesta para el desarrollo de un generador hardware de números aleatorios. La característica más relevante de la propuesta es el uso de conversión analógico -digital paralela para la obtención de datos de 12 bits.

El principio de operación empleado es el muestreo del ruido térmico proveniente de una juntura semiconductora. En este sentido se buscó la caracterización estadística y espectral del ruido proveniente de dos junturas diferentes. Las pruebas experimentales desarrolladas se proponen como una metodología estándar que debería seguirse al momento de validar el funcionamiento de un HRNG. Es claro que los problemas de esta clase de generadores son diferentes a los observados en los PRNGs, por lo tanto, es necesario desarrollar esquemas de solución apropiados para su tratamiento.

## REFERENCIAS


[1] Bo Dömstedt1, Jesper Jansson , "The Theory of Dynamic Encryption, a New Approach to Cryptography", Protego Information AB, Dept. of Computer Science, Lund University,2001.

[2] www.protocoltester.com

[3] Juan Soto," Statistical Testing of Random Number Generators", National Institute of Standards & Technology,2000.

[4] Stefan Wegenkittl , " Gambling tests for pseudorandom number generators ", institut fur mathematik , Universitat Salzburg, http://random.mat.sbg.ac.at, 2000.

[5] www.hotbits.com

[6] R. Davies, "Hardware random number generators",15th Australian Statitiscs Conference, july 2001.

[7] R. Davies, http://webnz.com/robert/hwrng.htm

[8] J. Leydold , H. Leeb , W. Hormann , " Higher Dimensional Properties of non-uniform pseudo random numbers " , Department for statistics WU Wien , ISOC University of Vienna , IE Department Bogazici, University Istanbul,1999.

[9] J. Proakis , D. Manolakis, Tratamiento digital de señales, PTR, , UK , 1998, pp 905-924,1998.

[10] A. Papoulis , " Probability , Random variables and stochastic processes " , PTR. , 1994.



**Miguel Melgarejo.**
Ingeniero Electrónico Universidad Distrital (2001), Grado de Honor Franciso José de Caldas. Profesor Facultad de Ingeniería U.D. Estudiante de Maestría en Ingeniería Electrónica y Computadores con énfasis en Microelectrónica, U. de los Andes. **mmelgarejo@ieee.org**

**Alexis Pirajan.**
Ingeniero Electrónico Universidad Distrital (2001). Profesor Facultad de Ingeniería U. Piloto de Colombia. Estudiante de Maestría y asistente graduado en Ingeniería Electrónica y Computadores con énfasis en Telecomunicaciones, U. de los Andes. **a-piraja@uniandes.edu.co**