COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

ANÁLISIS Y EVALUACIÓN DEL CIRCUITO GENERADOR DE NUMEROS ALEATORIOS *LAMPERT CIRCUIT*

Autor:

Alejandro Rodríguez García

Directores:

Dr. Gregorio López López

Dr. Javier Matanza Domingo

Madrid

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título "ANÁLISIS Y EVALUACIÓN DEL CIRCUITO GENERADOR DE NUMEROS ALEATORIOS LAMPERT CIRCUIT" en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico 2020/21 es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido

tomada de otros documentos está debidamente referenciada.

Fdo.: Alejandro Rodríguez García Fecha: 11/07/2021

Autorizada la entrega del proyecto

LOS DIRECTORES DEL PROYECTO

Fdo.: Dr. Gregorio López López Dr. Javier Matanza Domingo

Fecha: 11 / 07 / 2021

COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

ANÁLISIS Y EVALUACIÓN DEL CIRCUITO GENERADOR DE NUMEROS ALEATORIOS *LAMPERT CIRCUIT*

Autor:

Alejandro Rodríguez García

Directores:

Dr. Gregorio López López

Dr. Javier Matanza Domingo

Madrid

ANÁLISIS Y EVALUACIÓN DEL CIRCUITO GENERADOR DE NUMEROS ALEATORIOS LAMPERT CIRCUIT

Autor: Rodríguez García, Alejandro
Directores: Dr. Gregorio López López, Dr. Javier Matanza Domingo
Entidad Colaboradora: IIT- Universidad Pontificia Comillas y *University of Kent*

ABSTRACT

La generación de números aleatorios es crítica para los sistemas criptográficos modernos. En el marco del proyecto *Secure Internet of Things*, liderado por la Universidad de Stanford, se desarrolló un circuito generador de números aleatorios denominado *Lampert Circuit*. Este circuito se basa en electrónica sencilla y destaca por producir números aleatorios con alta entropía (0.98 bits/muestra) y por ser barato, pequeño y auditable, ideal, por tanto, para sistemas IoT. El objetivo de este trabajo de investigación es precisamente auditar su funcionamiento analizando 100 circuitos fabricados por 4 empresas distintas. De los resultados obtenidos se ha concluido que se trata de un RNG válido para aplicaciones criptográficas IoT pero el cual hay que evolucionar hacia un sistema de fácil implementación y más seguro. Finalmente, se han propuesto nuevas líneas de trabajo con el objetivo de dar continuidad al proyecto y contribuir al desarrollo de RNG que superen los retos del futuro.

Palabras clave: Entropía, Generación de Números Aleatorios, RNG, Ruido de avalancha, Zener, Criptografía.

1. Motivación y Objetivos

Los generadores de números aleatorios (RNG) juegan un papel fundamental dentro de los sistemas criptográficos modernos. A su vez la criptografía se ha convertido, dentro de las redes de comunicación modernas, en uno de los pilares fundamentales de la ciberseguridad. Sí además, le sumamos el hecho de que las nuevas tendencias tecnológicas actuales, como las redes IoT y computación cuántica plantean nuevos retos para los RNG, el interés por estos dispositivos queda más que justificado. Este interés lleva a los investigadores y empresas a proponer nuevos métodos o sistemas para generar números aleatorios cada año. Uno de los grandes problemas generales de estos estudios es que no suelen prestar tanta atención a la auditabilidad del RNG como al diseño y debido a esto muchas veces es complejo afirmar que un sea verdaderamente válido para criptografía. Por todo ello, este estudio pretende contribuir al desarrollo de RNG auditables, robustos, fiables y optimizados para entornos IoT.

En este estudio se ha replicado y complementado los test descritos en el artículo "*Robust, low-cost, auditable random number generation for embedded system security*" [1], publicado en ACM SenSys'16. Con el objetivo de adquirir resultados estadísticos fiables se han realizado las pruebas sobre un gran número de circuitos fabricados por diferentes empresas, para posteriormente analizar

los resultados obtenidos y compararlos con los del artículo original. De esta forma se pretende evaluar la idoneidad del circuito como generador de números aleatorios, así como discutir la viabilidad de una posible implementación en el entorno de IoT.

2. Metodología y Recursos

Para poder evaluar si el rendimiento del generador de números aleatorios depende del circuito utilizado y de su fabricante se han realizado las medidas sobre 100 unidades del *Lampert Circu*it. Se han encargado 25 circuitos de 4 fabricantes distintos: *European Circuits* (Reino Unido), *Wurth* (España), *Micron20* (Bulgaria) y *ShenZhenU2* (China). La Figura 1 muestra los circuitos fabricados.

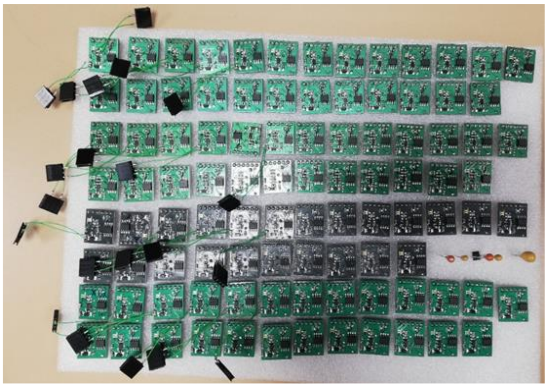


Figura 1: Conjunto de circuitos fabricados para la realización de las pruebas

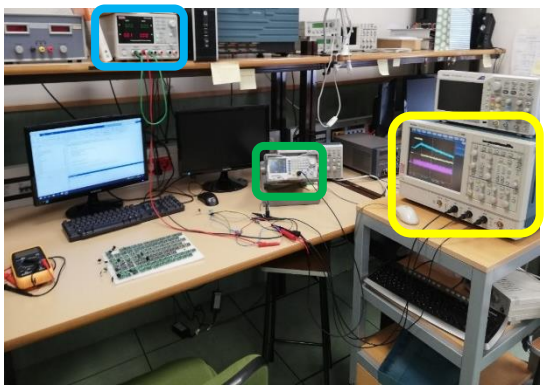


Figura 2: Laboratorio e instrumental disponible para llevar a cabo las pruebas

El proceso de replicación de las medidas no ha sido sencillo especialmente por la falta de documentación de cómo se realizaron en el artículo [1]. Debido a esto se han acabado realizando múltiples medidas que analizan un mismo aspecto del circuito, pero de las cuales cada una siguen un proceso de aprendizaje respecto a las medidas anteriores.

La Figura 2 muestra el laboratorio y el instrumental del que se dispone para llevar a cabo las pruebas: *Osciloscopio Tektronix TDS5104* (rodeado en amarillo en la Figura 2) conectado a la red LAN del laboratorio para poder procesar las medidas realizadas con MATLAB, el *Generador de Señales RIGOL DG1000Z* (rodeado en verde en la Figura 2), fuente de alimentación *Siglent SPD3303C* (rodeado en azul en la Figura 2).

3. Análisis sobre el funcionamiento interno

El primer problema que se encontró al replicar los experimentos fue las discrepancias entre los esquemáticos, la descripción de componentes incluida en el artículo y la versión disponible en el repositorio de GitHub [2]. Después de intercambiar varios correos con los autores, actualizaron la información relativa al circuito con el que se llevaron a cabo las pruebas descritas en el artículo en el repositorio de GitHub. La Figura 3 muestra el esquemático y los valores de los componentes utilizados.

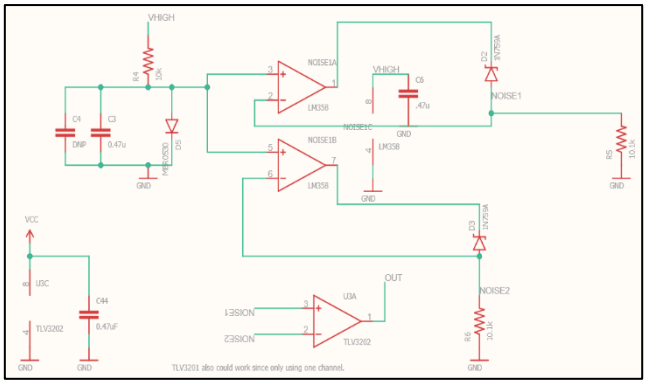
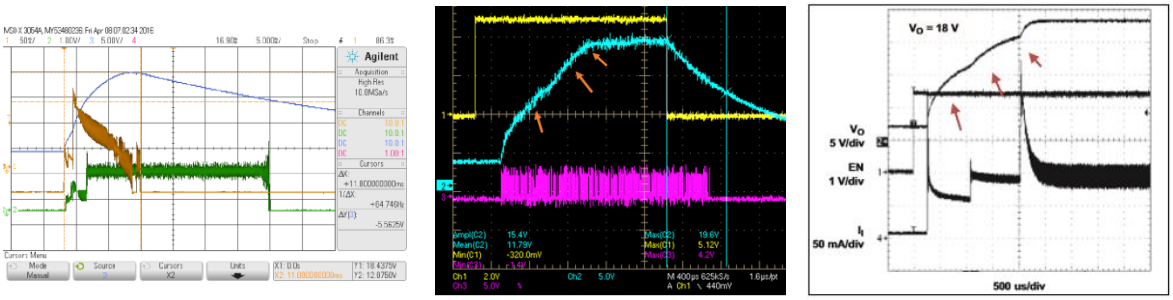


Figura 3: Esquemático de la PCB para los dos Generadores de Ruido y el comparador final

Siguiendo las referencias de la Figura 3, el circuito formado por R4, C3 y D5 sirve para fijar la tensión de referencia en la pata positiva de los operacionales LM358. El diodo usado para para la generación de ruido es el Zener 1N759A,que gracias a que se sitúa dentro de una realimentación negativa se encuentra constantemente en el proceso de avalancha a 12V. Las dos fuentes de ruido van al comparador TLV3202, donde se restan el nivel medio de ambas y la salida de dicho comparador (OUT) es la salida del generador de números aleatorios.

Para que el circuito funcione como se acaba de describir, es necesario polarizar el diodo Zener en inversa, por lo VHIGH debe ser superior a 12 V. Como la alimentación de los sistemas empotrados varía entre 1’8 y 3’3 V se utiliza un *boost converter* (implementado con TPS61041), que eleva la tensión por encima de 12V. El *boost converter* funciona en dos etapas periódicas controlado por una señal *enable*: un ciclo de carga en el que VHIGH alcanza 18V y una de descarga en la que baja hasta 12V. Es en esta etapa de descarga en la que en [1] especifican que hay que leer la salida aleatoria.



(a) (b) (c)

Figura 4: (a) Funcionamiento del boost converter indicado en [1]; (b) Funcionamiento medido en nuestro laboratorio; (c) Funcionamiento según el datasheet de TPS61041.

El segundo gran problema ha sido, por un lado, que la fase de carga no presenta la misma forma de onda (Figura 4.b) mostrada en [1] (Figura 4.a), aunque es coherente con el *datasheet* de TPS61041(Figura 4.c). Por el otro, la fase de descarga tiene una duración de diez veces menor que la descrita en el artículo (como se observa en la Figura 4.b) medida para 5 circuitos de cada fabricante.

Si tomamos el tiempo de descarga medido menor de 0’4ms y si usamos la frecuencia de muestreo recomendada en [1] (128kHZ) tendremos solo 51 bits por ciclo, frente a los 500-800 bits que se especifican en [1] se concluye que es insuficiente. Para prolongar la descarga, se ha incrementado la capacidad del condensador C2 hasta 10µF, obteniéndose tiempos de descarga de 30 ms.

En cuanto al análisis del diodo Zener como generador de ruido, se ha observado como el punto óptimo de máxima generación se produce para un rango reducido de la tensión de alimentación, entre 12’5V y 12’8V, mientras que en el artículo obtiene 12’16V. Finalmente, realizando mediadas sobre 10 diodos distintos, se ha concluido que dicha discrepancia es debida a que no todos los diodos se comportan igual y que cada uno tiene un punto óptimo de trabajo. Además, se ha comprobado que con la realimentación, aunque cada diodo tenga un punto de generación óptimo distinto, se corrige y no afecta al funcionamiento del circuito.

4. Análisis de la entropía y correlación de la salida aleatoria

En primer lugar, se ha replicado el análisis de la frecuencia óptima de muestreo que realizan en [1], donde se calcula la entropía y la correlación serie para distintas frecuencias. Se ha identificado como la máxima recomendable 1.25MHz, punto en la que el espectro de la señal pasa a ser completamente plano. Además, por encima de esta frecuencia, la correlación serie se dispara incrementando a medida que aumenta la frecuencia de muestreo aunque la entropía se mantiene (Figura 5 y 6). Para las frecuencias menores, la entropía se encuentra siempre por encima de 0’997 y la correlación serie por debajo de 0’03, valores buenos para conseguir una salida aleatoria. También se ha podido identificar la necesidad de evitar el diezmado en el postprocesado, ya que este afecta al nivel medio de las señales además de atenuarlas. Finalmente, es importante destacar que se ha identificado la filtración de la señal de un PLC del laboratorio en la salida aleatoria del circuito a través de la alimentación del circuito, si no se corrige podría dar lugar a futuros ataques con el objetivo de reducir la calidad de la secuencia aleatoria.

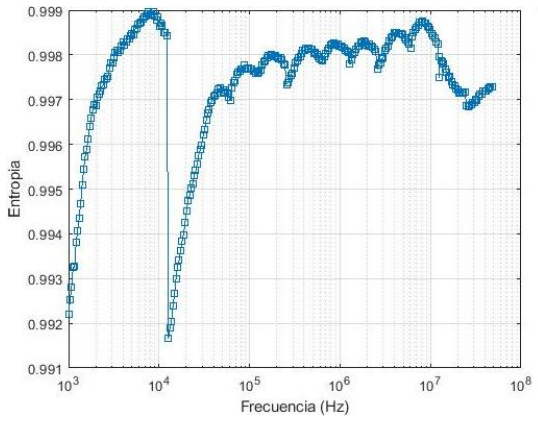


Figura 5: Entropía con nivel medio fijo a 1’65V desde múltiples frecuencias

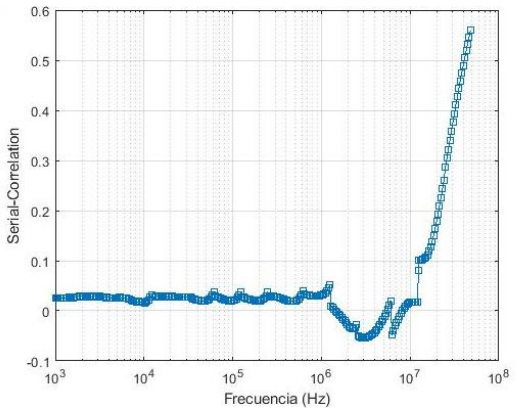


Figura 6: Correlación Serie con nivel medio fijo a 1’65V desde múltiples frecuencias

En segundo lugar, a raíz del análisis en frecuencia se consideró realizar las mediciones sobre el resto de los circuitos con una frecuencia de muestreo 125kHz, la más similar a la establecida en el artículo de 128kHz sin necesidad de diezmar en el postprocesado y que además cumple el criterio establecido en este estudio de ser menor que 1.25MHz. A raíz de las discrepancias en relación con el *boost converter*, se han estudiado dos casos: muestreando solo en la fase de descarga controlada con la señal *enable y* otro en la que el *boost converter* se ha mantenido siempre activado. Uno de los resultados principales es que no se han encontrado que las medidas con el *enable* siempre activado presenten resultados peores que las medidas únicamente en la fase de descarga (comparación entre la Figura 7 y 8). Tampoco se han encontrado sesgos entre los circuitos de cada fabricante, aunque si hay 3% de los circuitos que presentan un mal comportamiento y un 5% que venían mal de fabrica o dejaron de funcionar en el desarrollo de las medidas. En líneas generales se han obtenido resultados muy similares a los del artículo, con una entropía por encima de 0'97 y una correlación serie por bit menor (en valor absoluto) que ±0'002.

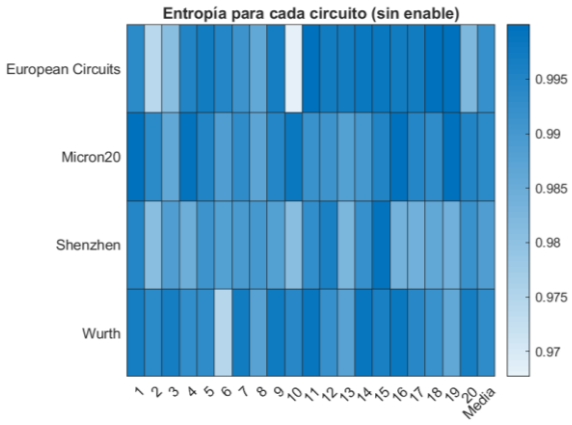


Figura 7: Entropía sin enable para 80 circuitos

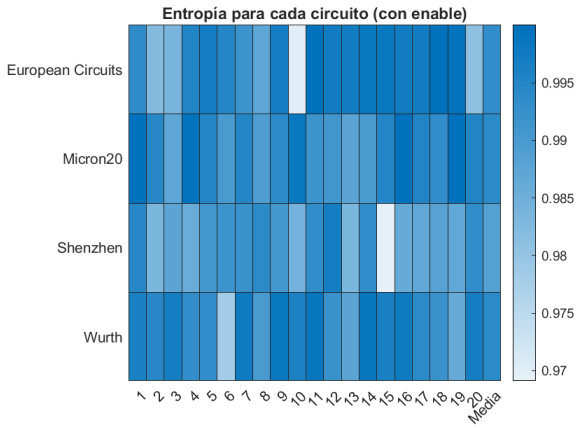


Figura 8: Entropía con enable para 80 circuitos

5. Conclusiones

En primer lugar, en cuanto a las discrepancias con respecto a lo descrito en el artículo [1] se han observado para circuitos de distintos fabricantes, en medidas tomadas en distintos entornos y con configuraciones diferentes, nos permite concluir que se trata de sesgos producidos por la forma en la que está concebido el circuito y no por un problema en la fabricación o en las tolerancias de los componentes. A pesar de dichas discrepancias se ha conseguido finalmente conseguir valores de entropía y correlación serie similares a los del artículo para una muestra significativa de circuitos.

En segundo lugar, no solo se han extraído conclusiones sobre el comportamiento del *Lampert Circuit*, también se ha tomado consciencia de que uno de los mayores retos de diseñar y auditar RNG es el gran número de ramas de conocimiento que se deben tener en cuenta (electrónica, radiación, procesamiento de señales, criptografía, estadística, etc.). En tercer lugar, se ha descubierto la complejidad que supone replicar de un estudio sobre un sistema hardware frente a los sistemas software. Dicha complejidad se explica en gran parte al gran número de factores que pueden afectar

en los resultados finales de las mediciones que los investigadores muchas veces no tienen en cuenta y no se documentan debidamente, una de las principales críticas que se le pueden hacer a [1]. En cuarto lugar, otra de las críticas que se le pueden hacer al *Lampert Circuit* es la dificultad de su implementación en una aplicación real, pues la salida del circuito es una señal analógica normalmente con valores intermedios (2V-1V). Esto no se puede leer directamente con entradas digitales, ya que no se asegura si se interpretará como un 0 o 1 lógico, por lo que se requiere hardware complejo.

Por último, a pesar de los puntos débiles del circuito, es necesario destacar que al comparar *Lampert Circuit* con otros RNG, destaca por la relación entre su sencillez frente a los buenos resultados de entropía y correlación que alcanza. En consecuencia, se considera un buen RNG que puede tener éxito en el entorno IoT, aunque necesita progresar en algunos aspectos.

La principal contribución de este estudio es la afirmación de que el *Lampert Circuit* puede ser un RNG válido para aplicaciones criptográficas IoT, pero el cual hay que evolucionar hacia un sistema de fácil implementación y más seguro. Además, se ha facilitado con la documentación y el código desarrollado en este estudio a futuros investigadores la auditabilidad del *Lampert Circuit* u otros RNG, lo cual ha generado interés tras su presentación en la JNIC del 2021. Motivados por lo expuesto en la JNIC y a raíz de las conclusiones de este estudio se plantean tres nuevas líneas de trabajo:

- Publicar el trabajo realizado junto con el código para establecer una base y metodología para llevar a cabo el analisis de hardware generador de números aleatorios en particular, y que permita reducir la complejidad de la replicabilidad de sistemas hardware en general.
- Continuar las mediciones sobre el circuito buscando posibles vulnerabilidades que puedan invalidar el circuito para aplicaciones criptográficas. Especialmente analizar como de vulnerable es ante ataques de introducción de señale a través de la red eléctrica. En paralelo al análisis de vulnerabilidades es necesario diseñar contramedidas que reduzcan sus efectos, como pueden ser etapas de filtrado que aíslen el circuito de la red.
- Facilitar la integración del circuito dentro de los sistemas criptográficos, especial dentro del entorno de las IoT. Se puede incorporar una etapa posterior a la salida aleatoria donde se digitalice usando un comparador sincronizado con una señal de reloj. Además, se plantea adaptar el sistema a plataformas como Arduino o Raspberry Pi para que el circuito pueda ser incorporado dentro de un gran número de proyectos.

6. Referencias

[1] B. Lampert, R.S. Wahby, S. Leonard, P. Levis, “Robust, low-cost, auditable random number generation for embedded system security,” *SenSys '16: Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems.* November 2016, Pages 16–27, doi: https://doi.org/10.1145/2994551.2994568

[2] GitHub Lampert Circuit: https://github.com/lampertb/LampertCircuitRNG

ANALYSIS AND EVALUATION OF THE RANDOM NUMBER GENERATOR LAMPERT CIRCUIT

Author: Rodríguez García, Alejandro
Directed by: Dr. Gregorio López López, Dr. Javier Matanza Domingo
Collaborating Entity: *IIT- Universidad Pontificia Comillas* and University of Kent

ABSTRACT

Random number generation is critical for modern cryptographic systems. Within the framework of the *Secure Internet of Things* project, led by Stanford University, a random number generator circuit called the *Lampert Circuit* was developed. This circuit is based on simple electronics and stands out for producing random numbers with high entropy (0.98 bits/sample) and for being cheap, small and auditable, ideal for IoT systems. The objective of this research is precisely to audit its operation by analyzing 100 circuits manufactured by 4 different companies. From the results of the research has been concluded that it is a valid RNG for IoT cryptographic applications, but which must progress towards an easy-to-implement and more secure system. Furthermore, new lines of work have been proposed in order to give continuity to the project and contribute to the development of RNG that will overcome the challenges of the future.

Keywords: Entropy, Random Number Generation, RNG, Avalanche Noise, Zener, Cryptography.

1. Motivation and Objectives

Random Number Generators (RNG) play a fundamental role in modern cryptography. In turn, cryptography has become, within modern communication networks, one of the essential pillars of cybersecurity. If we also include the fact that current technological trends, such as IoT networks and quantum computing raise new challenges for RNGs, the interest in these devices is more than justified. This interest leads researchers and companies to propose new methods or systems to generate random numbers every year. One of the common problems of these studies is that they do not pay enough attention to the auditability of the RNG as to the design. Because of this, it is often difficult to affirm that a RNG is valid for cryptography. Therefore, this study aims to contribute to the development of auditable, robust, reliable and optimized RNGs for IoT environments.

This study has replicated and complemented the tests described in the article "*Robust, low-cost, auditable random number generation for embedded system security*" [1], published in ACM SenSys'16. With the aim of acquiring reliable statistical results, tests have been carried out on a large number of circuits manufactured by different companies, to later analyze the results obtained and compare them with those of the original article. With this, it is intended to evaluate the suitability of

the circuit as a random number generator and discuss the feasibility of a possible implementation in the IoT environment.

2. Methodology and Resources

In order to evaluate whether the performance of the random number generator depends on the circuit used and its manufacturer, measurements have been made on 100 units of the *Lampert Circuit*. 25 circuits have been ordered from 4 different manufacturers: *European Circuits* (UK), *Wurth* (Spain), *Micron20* (Bulgaria) and *ShenZhenU2* (China). Figure 1 shows all the circuits tested.

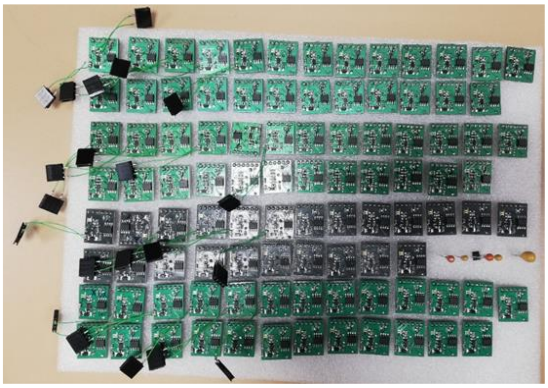


Figure 1: Circuits manufactured to carry out the tests

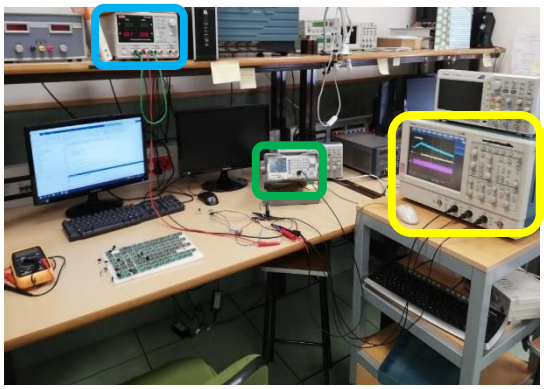


Figure 2: Laboratory and instruments necessary to carry out the tests

The process of replicating the measures has presented some complications, especially due to the lack in the documentation of how they were carried out in [1]. Due to this, multiple measurements that analyze the same aspect of the circuit have been carried out. but of which each one follows a learning process with respect to the previous measurements.

Figure 2 shows the laboratory and the instruments available to carry out the measures: *Tektronix TDS5104 oscilloscope* (surrounded in yellow in Figure 2) connected to the LAN of the laboratory to be able to process the measurements with MATLAB scripts on the lab computer, the *Generator of RIGOL DG1000Z Signals* (surrounded in green in Figure 2), *Siglent SPD3303C power supply* (surrounded in blue in Figure 2).

3. Analysis of the internal circuit behaviour

The first problem that was found when replicating the experiments was the differences between the schematics, the description of components included in the article and the version available in the GitHub repository [2]. After exchanging several emails with the authors, they updated in the GitHub repository the information of the circuit used in the article to carry out the test. Figure 3 shows the schematic and the values of the components used.

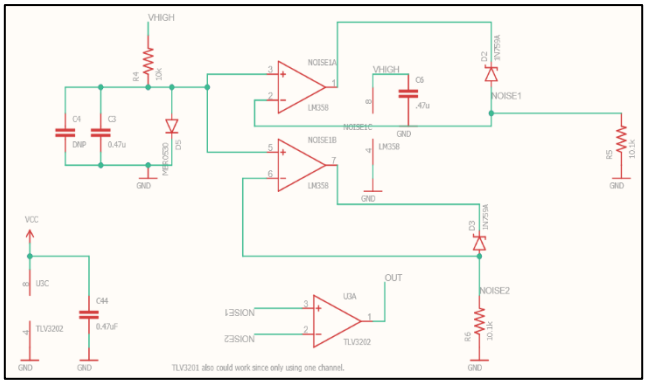
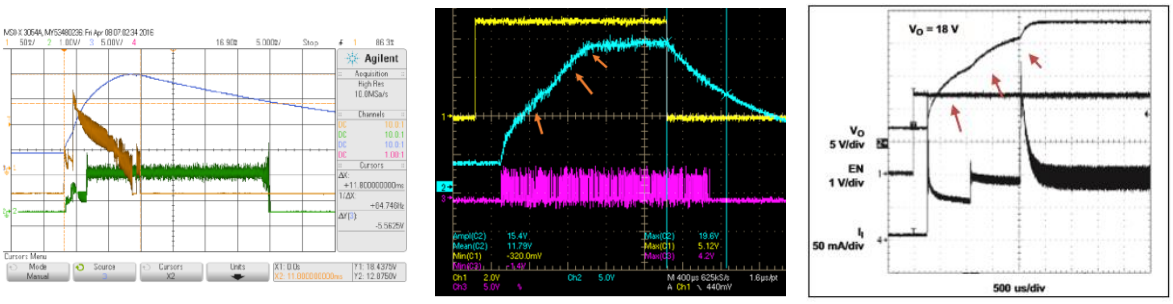


Figure 3: PCB schematic of the two noise generators and the final comparator

Using the same notation as in Figure 3, the circuit formed by R4, C3 and D5 set the reference voltage on the positive pin of the LM358 operational. The diode used for noise generation is the Zener 1N759A, which thanks to its negative feedback is constantly in the avalanche process at 12V. The two sources of noise go to the comparator TLV3202, where average level of both is subtracted and the output of TLV3202 (OUT) is the output of the random number generator.

The circuit only work as described above, the Zener diode must be reverse biased and VHIGH must be higher than 12V. Because the power supply for embedded systems is normally in the range of 1'8V and 3'3V, a *boost converter* is used (implemented with TPS61041), which raises the voltage above 12V. The boost converter works in two periodic stages controlled by an enable signal: a charge cycle in which VHIGH reaches 18V and a discharge cycle in which it drops to 12V. It is in this discharge stage where the random output must be read only, as specified in [1].



(a) (b) (c)

Figure 4: (a) Performance of the boost converter indicated in [1]; (b) Performance measured in our laboratory; (c) Performance according to the TPS61041 datasheet.

The second major problem has been with the *boost converter*. First, was identified that the charging phase does not present the same waveform (Figure 4.b) shown in [1] (Figure 4.a), although it is consistent with the TPS61041 datasheet (Figure 4.c). Secondly, was measure that the discharge phase lasts ten times less than that described in the article (as seen in Figure 4.b) measured for 5 circuits of each manufacturer.

If we take the measured shortest discharge time, of 0’4ms, and if we use the sampling frequency recommended in [1] (128kHZ) we will have only 51 bits per cycle, compared to the 500-800 bits specified in [1] it was concluded that the duration is insufficient. To increase the discharge time, the capacitor C2 has been increased to 10µF, obtaining discharge times of 30ms.

Finally, a third discrepancy was identified in the analysis of the Zener diode as a noise generator. It has been observed that the optimum point of maximum generation occurs for a reduced range of the supply voltage, between 12'5V and 12'8V, while in the article it obtains 12 '16V. Finally, carrying out measurements on 10 different diodes, it has been concluded that the discrepancy is produce because not all diodes behave the same and each diode has a different optimum working point. In addition, it has been verified that with the feedback, although each diode has a different optimal generation point, it is corrected and does not affect the operation of the circuit.

4. Analysis of entropy and correlation of aleatory output

First, the analysis of the optimal sampling frequency carried out in [1] has been replicated, where entropy and serial correlation are calculated for different frequencies. 1’25MHz was identified as the maximum sampling frequency recommended, is the point where the signal spectrum becomes completely flat. Furthermore, above this frequency, the serial correlation increases as the sampling frequency increases, although the entropy is maintained (Figures 5 and 6). For the lower frequencies, the entropy is always above 0'997 and the serial correlation below 0'03, good values to get a random output. It has also been possible to identify the need to avoid decimation in post-processing, since this affects the average level of the signals and produce attenuating in the random signal. Finally, it is important to highlight the filtration of signals from a laboratory PLC in the random output of the circuit through the power supply, if this is not rectified it could lead to future attacks with the aim of reducing randomness.

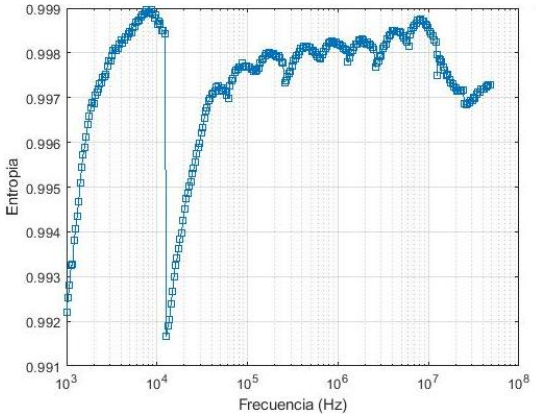


Figure 5: Entropy with fixed mean level at 1.65V from multiple frequencies

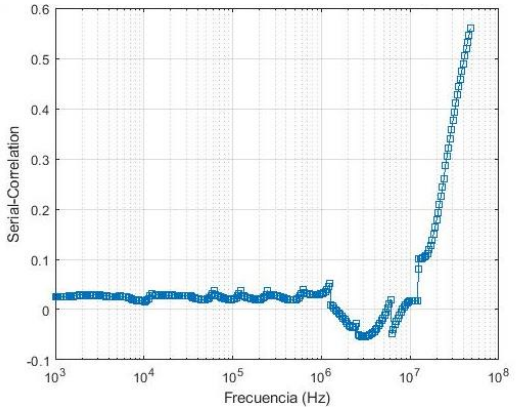


Figure 6: Serial correlation with fixed mean level at 1.65V from multiple frequencies

Secondly, as a result of the frequency analysis, was considered to carry out the measurements on the rest of the circuits with a sampling frequency of 125kHz, because is the most similar to that the one established in the article of 128kHz without the need to decimate in the post-processing and also because it complies with the criterion established in this study of using a frequency lower than 1.25MHz. As a result of the discrepancies in relation to the *boost converter*, two cases have been studied: sampling only in the discharge phase controlled with the *enable* signal and another in which the boost converter has always remained activated. One of the main results is that measurements with the *enable* always active have not been found to present worse results than measurements only in the discharge phase (comparison between Figure 7 and 8). Nor have been found biases between the circuits of each manufacturer, although there are 3% of the circuits that present a bad behavior and 5% that came badly from the factory or stopped working in the development of the measures. In general, the results are very similar to the ones of the article, with an entropy above 0.97 and a serial correlation per bit lower (in absolute value) than ± 0.002.

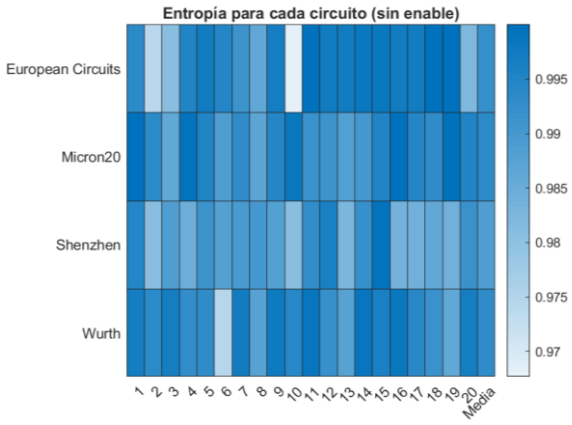


Figure 7: Entropy without enable for 80 circuits

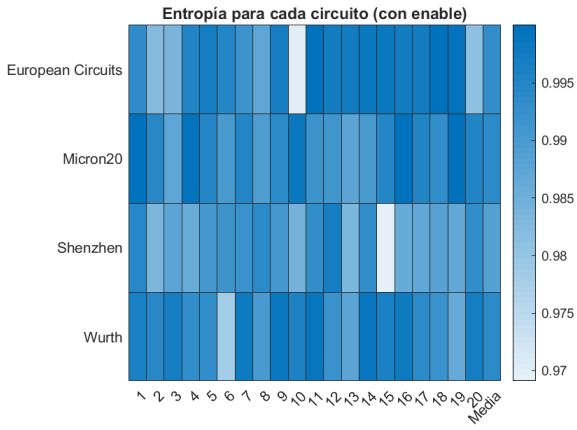


Figure 8: Entropy with enable for 80 circuits

5. Conclusions

First of all, regarding the discrepancies with what is described in article [1], they have been observed for circuits from different manufacturers, in measurements taken in different environments and with different configurations. Consequently, it allows us to conclude that these are biases produced by the way the circuit is designed and not because of problems in manufacturing or in component tolerances. Despite these discrepancies, it has finally been possible to achieve values of entropy and series correlation similar to those of the article for a significant sample of circuits.

Secondly, not only conclusions have been drawn about the behavior of the *Lampert Circuit*, but it has also been concluded that one of the greatest challenges of designing and auditing RNG is the large number of knowledge branches that must been considered (electronics, radiation , signal processing, cryptography, statistics, etc.). Thirdly, the complexity involved in replicating a study of a hardware system is much bigger than software systems. This complexity can be explained by the large number of factors that can affect the final results of the measures that researchers often do not

consider and are not properly documented. This is one of the main criticisms that can be made to [1]. Fourthly, another criticism that can be made to the *Lampert Circuit* is the difficulty of its implementation in a real application, since the output of the circuit is an analog signal that most of the time is in intermediate values (2V -1V). This cannot be read directly with digital inputs, as it is not certain whether it will be interpreted as a logical 0 or 1 and complex hardware is required.

Finally, despite the circuit's weak points, it should be noted that after comparing the *Lampert Circuit* with other RNGs, stands out for the relation between its simplicity and the good results of entropy and correlation it achieves. Consequently, it is considered a good RNG that can be successfully implemented in the IoT environment, although it needs to progress in some aspects.

The main contribution of this study is that the *Lampert Circuit* can be a valid RNG for cryptographic IoT applications, but which has to progress towards an easy-to-implement and secure system. In addition, the auditability methodology of the *Lampert Circuit*, applicable to other RNGs, has been provided with the documentation and code developed in this study to future researchers. This project has generated interest after its presentation at the JNIC in 2021. Motivated by what was stated in the JNIC and as a result from the conclusions of this study, three new lines of work are proposed:

- Publish the work carried out with the code to establish a methodology to carry out the analysis of hardware random number generator in particular, and to reduce the complexity of the replicability of hardware-based proposals in general.
- Continue with the measures on the circuit, looking for possible vulnerabilities that could invalidate the circuit for cryptographic applications. Especially analyze how vulnerable it is to attacks of introduction of signal through the electrical network. In parallel to the vulnerability analysis, it is necessary to design countermeasures that reduce their effects, such as filtering stages that isolate the circuit from the network.
- Facilitate the integration of the circuit within cryptographic systems, especially within the IoT environment. A stage after the random output can be incorporated, where it is digitized using a comparator synchronized with a clock signal. In addition, it is proposed to adapt the system to platforms such as Arduino or Raspberry Pi so that the circuit can be incorporated into a large number of projects.

6. References

[1] B. Lampert, R.S. Wahby, S. Leonard, P. Levis, “Robust, low-cost, auditable random number generation for embedded system security,” *SenSys '16: Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems.* November 2016, Pages 16–27, doi: https://doi.org/10.1145/2994551.2994568

[2] GitHub Lampert Circuit: https://github.com/lampertb/LampertCircuitRNG

Índice de la memoria

Índice de figuras

Índice de tablas

Capítulo 1. INTRODUCCIÓN

En este trabajo fin de grado se evalúa experimentalmente el rendimiento del circuito generador de números aleatorios *Lampert Circuit*, desarrollado en el marco del proyecto *Secure Internet of Things* liderado por la Universidad de Stanford. Para ello se pretende replicar los test descritos en el artículo "*Robust, Low-cost, Auditable Random Number Generation for embedded system security*" [1], publicado en ACM SenSys'16, sobre un gran número de circuitos fabricados por diferentes empresas para posteriormente analizar los resultados obtenidos y compararlos con los del artículo original. Se busca contribuir al desarrollo y auditoría de generadores de números aleatorios (RNG) diseñados para entornos IoT (*Internet of Things*).

1.1. MOTIVACIÓN DEL PROYECTO

Durante la fase de documentación previa al desarrollo de las mediciones (descrita en el Capítulo 2) ha quedado al descubierto la importancia que tienen los RNG dentro de los sistemas criptográficos modernos. A su vez, se ha comprobado el papel tan importante que juega la criptografía dentro de las redes de comunicación modernas, constituyendo uno de los pilares fundamentales de la ciberseguridad. Debido a esto, en parte, se justifica el interés que existe en el diseño, desarrollo, implementación y análisis de nuevos RNG; no sólo por la comunidad científica, sino también por parte de gobiernos y grandes agencias reguladoras de seguridad.

Por otro lado, si hacemos un ejercicio de análisis de cuáles son las tendencias tecnologías actuales podemos incluir dentro de las más importantes las redes IoT y la computación cuántica. Ambas son tecnologías que siguen en desarrollo, que sin duda formarán parte de las redes de comunicación modernas y que plantean un nuevo reto para la ciberseguridad. La primera tecnología, las redes IoT, implican un incremento significativo en el número de dispositivos conectados en red, los cuales se encuentran constantemente recogiendo, almacenando y comunicando datos sensibles de los usuarios. Además, dichos dispositivos se encuentran especialmente expuestos a cualquier atacante tanto a nivel físico como a nivel de transmisión de los datos. Por ello, supone un gran reto para el objetivo de la criptografía conseguir comunicaciones seguras, manteniendo las limitaciones de tamaño y consumo de energía intrínsecas a estos dispositivos.

En cuanto a la segunda tecnología, la computación cuántica, aunque quedan años de investigación antes de su posible implementación en la red, se anticipa que su implementación supondrá un cambio de paradigma dentro del mundo tecnológico. Y es que, mientras que en un ordenador tradicional aumentar el número de bits no supone un incremento importante en su capacidad, en el caso de la computación cuántica, gracias al principio de superposición cuántica, cada qubit añadido supone un crecimiento exponencial en la capacidad. De esta forma, un texto encriptado que a un ordenador actual le puede llevar años descifrarlo, un ordenador cuántico puede tardar segundos en descifrarlo. En consecuencia, impera la necesidad de disponer de RNG capaces de generar, con un ratio elevado, claves lo suficientemente aleatorias y largas para cuando este día llegue.

Como ya se indicaba en el primer párrafo, el interés sobre los RNG es alto y aunque no sea un campo de investigación novedoso, ya que desde mediados del siglo XX se han ido realizando numerosas contribuciones, lo cierto es que las necesidades actuales llevan a la publicación de RNG nuevos y muy diversos cada año. Uno de los grandes problemas en estos estudios es que en muchos no se le da tanta importancia al análisis de la aleatoriedad de sus diseños o a la comparación de su propuesta con otras publicadas. Por ello, este estudio pretende contribuir al desarrollo de nuevos RNG auditables, robustos, fiables y optimizados para entornos IoT.

1.2. OBJETIVOS

Movido por las motivaciones expuestas en el apartado anterior, el objetivo de este Trabajo Fin de Grado es evaluar tanto experimentalmente como de forma teórica el rendimiento del circuito RNG conocido como *Lampert Circuit*. Dicho circuito ha sido desarrollado en el marco del proyecto "*Secure Internet of Things*", liderado por la Universidad de Stanford.

Por un lado, se pretende realizar un análisis teórico del funcionamiento del *Lampert Circuit*, así como una comparación con el resto de los generadores publicados en los últimos años, prestando especial atención a los requisitos que deben tener en el entorno de IoT.

Por el otro, se van a replicar y complementar los test descritos en el artículo "*Robust, low-cost, auditable random number generation for embedded system security*" [1], publicado en ACM SenSys'16. Con el objetivo de adquirir resultados estadísticos fiables se van a realizar las pruebas sobre un gran número de circuitos fabricados por diferentes empresas, para posteriormente analizar los resultados obtenidos y compararlos con los del artículo original. De esta forma se

pretende evaluar la idoneidad de dicho circuito como generador de números aleatorios, así como discutir la viabilidad de una posible implementación del RNG en el entorno de IoT.

1.3. ESTRUCTURA DE LA MEMORIA

La memoria se divide en 8 capítulos que se pueden agrupar en 4 bloques. El primero conformado por el *Capítulo 1*, el *Capítulo 2* y el *Capítulo 3*, se centra en describir las cuestiones generales sobre el trabajo realizado, así como a poner en contexto a los RNG. En concreto, en el *Capítulo 2*, se realiza un análisis detallado de los avances científicos relativos a los RNG. Primero en el punto *2.1.* se describe la base de la criptografía moderna y la relevancia de los números aleatorios para ésta. En el *2.2.* se explica la complejidad de testear la aleatoriedad y las alternativas para hacerlo. Por último, en el *2.3.* se describen los tipos de RNG, sus ventajas y debilidades, y donde encaja el *Lampert Circuit* dentro de estos. En el *Capítulo 3* se concreta el trabajo realizado en este estudio, incluyendo la metodología usada, los recursos materiales, la planificación y la estimación económica, diferenciando entre costes materiales y humanos.

El segundo bloque, formado por el *Capítulo 4* y *Capítulo 5*, contiene un análisis detallado del diseño del circuito y de su implementación. En primer lugar, la sección *4.1.* se analiza el *boost converter* comparando la descripción realizada en el artículo, con la del *datasheet* del integrado usado y la implementación subida a GitHub por los autores. En segundo lugar, en la sección *4.2.* se analiza el funcionamiento de los componentes involucrados en la generación del ruido y el funcionamiento de la realimentación. Finalmente, la sección *4.3.* se analiza el funcionamiento del comparador final que combina las dos fuentes de ruido. En el *Capítulo 5* se describen los componentes y las características de fabricación usados para el estudio.

El tercer bloque contiene la justificación, metodología y resultados de las medidas realizadas en el laboratorio. Todas las medidas se recogen en el *Capítulo 6*, donde se agrupan en cuatro apartados: el *6.1.* con las medidas sobre el *boost converter*, el *6.2* con medidas de las fuentes de ruido, el *6.3.* con medidas de la salida aleatoria para distintas frecuencias y, por último, el *6.4.* con medidas de correlación serie y entropía a la salida para la muestra significativa de circuitos.

En el último bloque, correspondiente con el *Capítulo 7*, se concluye la memoria con conclusiones sobre los experimentos realizados, conclusiones generales sobre los RNG, las contribuciones que realiza este estudio y los trabajos futuro.

Capítulo 2. ESTADO DE LA CUESTIÓN

Los números aleatorios son ampliamente conocidos dentro del ámbito académico por sus múltiples aplicaciones [2]. Se suelen utilizar en simulaciones en las que se pretende predecir distintos resultados que se ven afectados por procesos naturales con una componente aleatoria. También, se emplean para realizar muestreos de forma imparcial en estudios sobre una población. Por otro lado, son muy usados en la implementación de algoritmos cuando se quiere ejecutar una serie de instrucciones de forma aleatoria, como es el caso de muchos videojuegos en los que se busca darle al usuario una respuesta no lineal y que, por lo tanto, no sea la misma cuando se juega varias veces. Sin embargo, su uso se encuentra mucho más extendido de lo que nos pensamos y los usamos a diario, eso sí, de forma completamente indirecta.

2.1. CRIPTOGRAFÍA

Lo cierto es que los números aleatorios son uno de los pilares fundamental de la criptografía, la cual tiene como objetivo permitir que dos personas puedan intercambiar información de forma confidencial y segura usando un canal inseguro [3]. Otros autores definen el objetivo de la criptografía como el de construir esquemas o protocolos que puedan realizar ciertas tareas incluso en presencia de un adversario [4].

Aunque el inicio de la criptografía se remonta hasta el inicio de las primeras grandes civilizaciones, lo que conocemos como criptografía moderna surge a mediados del siglo XX cuando Shannon publicó su artículo *"Communication Theory of Secrecy Systems"* [5], en el que establece los principios teóricos de los sistemas secretos.

En primer lugar, [5] define el concepto de sistema secreto como un conjunto de transformaciones de un espacio a otro. Cada una de las transformaciones es resultado de usar una clave de cifrado particular y tienen que ser reversibles de tal forma que sólo se pueda descifrar si se conoce la clave. De esta forma se establece que la probabilidad de que se realice una transformación está directamente relacionada con la probabilidad de escoger un determinada clave. Dichas probabilidades son las que determinan las probabilidades de acierto de un atacante criptoanalista que pretende descifrar un mensaje cifrado. Por otro lado, se estudia como un enemigo puede capturar un criptograma para calcular a través de él las probabilidades de los

próximos mensajes y claves, con el objetivo de decodificar la encriptación de mensajes posteriores.

En segundo lugar, responde a la pregunta de cómo de seguro es un sistema si el criptoanalista dispone de tiempo y recursos ilimitados para descifrar un sistema seguro. La solución fue un sistema dotado de *Perfect Secrecy*. Lo definió como la cualidad de un sistema que para todos los textos claros introducidos *a* y todos los textos cifrados *b* la probabilidad de que se cifre *a* es igual a la probabilidad de que se haya cifrado *a* sabiendo que el texto cifrado resultante es *b*, es decir, $p(a)=p(a/b)$. Esto implica que un texto cifrado no aporta información alguna sobre su texto original. Para conseguirlo demostró matemáticamente que es posible si existen tantas posibles claves como mensajes se envíen, lo que implica que si se quieren enviar mensajes cada cierto periodo de tiempo la frecuencia de generación de claves debe ser mayor o igual.

En tercer lugar, se centra en analizar el *Practical Secrecy*, realizando un análisis de las debilidades básicas de un sistema secreto, concluyendo con una serie de métodos para implementar sistemas seguros que requerirán de una gran cantidad de recursos por parte de un atacante para descifrarlos.

Centrándonos en el diseño de RNG, de los principios establecidos en *Communication Theory of Secrecy Systems* [5] se han extraído cuatro conclusiones:

- Es imprescindible que exista equiprobabilidad de generar cada una de las posibles claves. Como explica Shannon, un criptoanalista se dedica a analizar las probabilidades de aparición de los símbolos dentro de los fragmentos cifrados interceptados. Si la equiprobabilidad de las claves no se cumple, el atacante podrá adquirir conocimiento del sistema. De este modo puede ser capaz de predecir la encriptación de mensajes posteriores.
- Para poder aproximarse lo máximo posible al secreto perfecto es necesario que el ratio de generación de claves sea lo más alto posible, buscando alcanzar una longitud de clave igual o mayor que la longitud del texto claro.
- Es necesario que las claves generadas no guarden relación entre sí, debido a que si se puede estimar una clave generada a partir de las anteriores, por muchas técnicas de confusión que se implementen en el algoritmo de cifrado, los textos cifrados consecutivos pueden guardar relación entre sí que un criptoanalista puede explotar.
- Podemos anticipar que los requisitos de aleatoriedad para un RNG, que se quiera utilizar en criptografía, serán de los más exigentes en comparación a los necesarios para otras aplicaciones.

En cuanto a las publicaciones actuales sobre criptografía, coinciden en que la eficacia de estos sistemas reside, en gran parte, en la calidad del generador de claves y que un RNG con déficits puede provocar un fallo de todo el sistema [6]. Por un lado, esta afirmación se basa en que lo que permite que un mensaje sea secreto usando los algoritmos criptográficos actuales no es el algoritmo como tal, ya que estos son conocidos, si no la clave que se usa para la encriptación. Por el otro lado, al diseñar los protocolos de seguridad usados en la red uno de los conceptos más importantes es la conocida como *Chain of Trust*, que hace referencia a que, si una parte del sistema se ve comprometida, el sistema entero se encuentra comprometido. De esta forma se puede justificar que, aunque sea muy seguro el uso de algoritmos criptográficos, sin las claves adecuadas se ve comprometido todo el sistema.

En la actualidad se puede alegar que la criptografía moderna se ha convertido en la principal herramienta de las comunicaciones seguras a través de internet, permitiendo implementar métodos de autentificación y transmisión de mensajes privados mediante el intercambio de claves [7]. Si a esta afirmación le sumamos que los RNG son la base de la pirámide de las arquitecturas de criptosistemas, podemos concluir que la generación de números aleatorios es un tema de gran interés en la comunidad científica. Prueba de ello es que el estudio y la implementación de sistemas generadores de números aleatorios han sido campos de investigación desde hace muchos años.

2.2. ALEATORIEDAD Y TEST

El concepto de aleatoriedad es quizás uno de los puntos más polémicos dentro de los estudios realizados sobre los generadores de números aleatorios, porque el hecho de que una secuencia de números sea o no aleatoria no es un criterio binario a través del cual se pueda determinar si un conjunto de números es aleatorio, sino que se trata de un conjunto de parámetros estadísticos que determinan su calidad. De este modo, para cada aplicación se establecen criterios distintos para determinar que una secuencia de números es suficientemente aleatoria. Por ello, en aplicaciones como pueden ser los videojuegos la calidad de la aleatoriedad no se le da tanto peso como a factores como la capacidad de procesamiento necesaria para generar secuencias aleatorias. Sin embargo, en el caso de la criptografía tener números aleatorios impredecibles juega un papel muy importante. Por eso en este apartado nos centraremos en los requisitos de aleatoriedad para un sistema criptográfico.

Aunque no exista un criterio único para analizar la aleatoriedad, a lo largo de los años se han ido realizando distintas aproximaciones a la cuestión. En *The Art of Computer Programming* [2] se recogen varios algoritmos generadores de números aleatorios y se proponen una serie de test para estudiar si las secuencias se comportan como aleatorias. En primer lugar, analiza dos procedimientos estadísticos generales para el estudio de números aleatorios: los *Chi-square tests* y *Kolmogorov-Smirnov tes*t(K-S test). Ambos son métodos estadísticos con los que se obtiene la probabilidad de rechazar la hipótesis nula.

En segundo lugar, propone una serie de test empíricos: *Equidistribution test (Frequency test)*, para analizar si los números se encuentran distribuidos de forma uniforme entre el cero y el uno con K-S test, *Serial test*, para analizar si los pares de números son independientes y se distribuyen de manera uniforme con un Chi-square test, *Gap test*, para determinar lo significativo que es el intervalo definido por la repetición de un mismo dígito, así hasta 11 test que estudian distintas cualidades de la aleatoriedad.

En tercer lugar, propone test teóricos, los cuales se centran en analizar la calidad los generadores de números aleatorios antes de su implementación, es decir, antes de que se obtenga una secuencia de números aleatorios con ellos. En cuarto lugar, analiza los *Spectral Test* centrados en la comprobación de la calidad de la aleatoriedad para los generadores del tipo *Linear Congruential* (LCG).

En resumen, *The Art of Computer Programming* [2] en su capítulo 2 realiza una recopilación detallada, tanto de múltiples algoritmos para la generación de secuencias aleatorias, como de métodos para analizar la aleatoriedad. Aunque desde el punto de vista estadístico y matemático el análisis realizado es de lo más completo, se centran en aplicaciones puramente computacionales a nivel de algorítmica.

Como ya se explicó con anterioridad en este estudio nos focalizaremos en los criptosistemas, por ello vamos a analizar otras propuestas especializadas en determinar la calidad de los RNG dentro de esta categoría. Uno de los análisis que más se utilizan es el propuesto como **NITS SP 800-22** [8], publicado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos. Algunos ejemplos de artículos sobre RNG en los que se utiliza son [9], [10], [11], [12], [13] entre otros. Dicho análisis está formado por 15 pruebas individuales (muchas de ellas similares a las expuestas en [2]) basadas en métodos estadísticos con los que evalúan la probabilidad de que un parámetro sea viable (p-valor) dada una hipótesis cierta, en nuestro caso que la secuencia sea

aleatoria. Para discernir si la hipótesis es cierta, se asigna un nivel de significación determinado. En criptografía se suele asignar un valor de 0.01 [14] que es a su vez el que establecen en [8].

Otro conjunto de pruebas ampliamente usado son los test **Diehard** [15], los cuales son un conjunto de 12 test estadísticos en los que tambien se usa un p-valor para determinar la aleatoriedad. Sin embargo, en este caso el nivel de significación no es un único valor, sino que es un rango (0.01-0.99) y aquellas mediciones que entren dentro del rango habrán superado el criterio de aleatoriedad [14]. Diehard son unas de las pruebas más estrictas para analizar la aleatoriedad. El principal problema es que no define un nivel significativo fijo, por lo que cada autor fija un p-valor determinado dependiendo de la precisión que quiera obtener [16]. Algunos estudios sobre RNG donde se usan las pruebas Diehard son [14] [16] [17] [18]. En ellos se usan para complementar a otras pruebas y asegurar que los números generados son óptimos. También, existen los test **Dieharder** [19]**,** una versión más moderna de los test Diehard en la que incluye nuevos test estadísticos como los propuesto en NITS SP 800-22.

TestU01 [20] es una librería de C publicada en 2007 en la que se implementan las pruebas estadísticas más usadas para analizar la aleatoriedad, así como algunos diseñados por los autores. Además, implementa algoritmos para la generación de números pseudoaleatorios. Hay que indicar que esta librería cuenta con una gran variedad de pruebas.

Por otro lado, existen estándares basados en pruebas que pueden ser implementadas en módulos hardware fácilmente. El más usado es **FIPS 140-2** [21]. Estas implementaciones en hardware son de gran utilidad para testear los chips con RNG producidos a gran escala o los basados en PUF (*Physical Unclonable Function*) [22]. FIPS 140-2 contiene cuatro pruebas independientes, pudiendo configurar niveles de significación distintos para cada test, por ejemplo, en función de la longitud de la secuencia analizada. FIPS 140-2 es un estándar muy usado entre empresas privadas que desarrollan módulos criptográficos, ya que se trata del estándar de requerimientos de seguridad de módulos criptográficos actual aprobado por el gobierno de los Estados Unidos [23].

Hay que destacar también que dentro del ámbito de la generación de números aleatorios uno de los proyectos más completos desarrollado por la NIST es el denominado "Random Bit Generation" (RGB) [24]. Dentro de este proyecto se encuentra la publicación de NITS SP 800-22 Rev. 1a [8] en 2010, pero sus desarrollos más recientes que siguen vigentes son:

- **SP 800-90A Rev. 1** [25] en 2015, donde se especifican mecanismos de generación mediante métodos determinísticos (DRGB).
- **SP 800-90C (Draft)** [26] en 2016, donde se exponen líneas de diseño y requerimientos de fuentes de entropía como fuente de los DRGB, así como una serie de test para validar su calidad.
- **SP 800-90B** [27] en 2018, donde se especifica una arquitectura para combinar las fuentes de entropía con los DRGB especificados en SP 800-90A y 800-90C.

Estos documentos no recogen un estándar como es el caso de FIPS 140-2 [21], sino que se trata de recomendaciones para el desarrollo de los RGB. Además, se ha observado como no se recurre tanto a ellos en publicaciones científicas como si es el caso de NITS SP 800-22 [8], quizás por ser más recientes o porque la código fuente de las pruebas propuestas no se encuentran disponible de manera oficial por la NIST, por lo que son los investigadores los que las tienen que implementar. Algunos estudios sobre diseños de RNG en los que se han usado son [28], [29] y [30].

Entrando más en detalle sobre el contenido de SP 800-90B [27], vemos cómo usa el concepto de entropía como base para el análisis de la calidad del ruido. En primer lugar, para medir la entropía usa la conocida como *min-entropy*, uno de los criterios más conservadores para medir la imprevisibilidad de los valores aleatorios generados. Dicho método de cálculo difiere del método clásico propuesto por Shannon [31], pero permite establecer criterios más estrictos para aplicaciones criptográficas, por lo que su valor será siempre menor que la de Shannon.

En segundo lugar, en el apartado "*2.2 The Entropy Source Model*", define las interfaces generales del sistema. Como muestra la figura 1, incluye un bloque de generación del ruido analógico, uno de digitalización a continuación, seguido por un bloque opcional de acondicionamiento en el que se aplican funciones deterministas para reducir sesgos y/o aumentar la entropía de la salida. Por último, se añade un bloque llamado *Health Test* en paralelo en el que se comprueba periódicamente que la salida sea óptima.

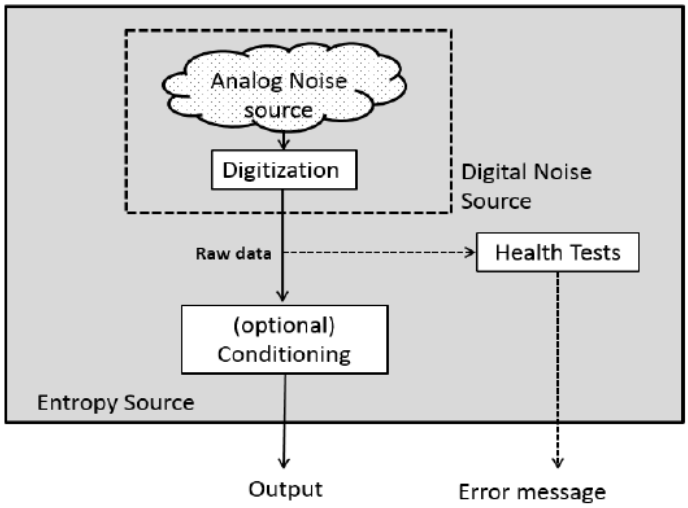


Figura 1: Esquema de una fuente de entropía propuesto en [23]

En tercer lugar, en el capítulo 3 de SP 800-90B [27], se define todo el proceso de validación del sistema de generación, estableciendo una serie de requerimientos para la fuente de entropía (que sería la salida final del sistema), para la fuente de ruido (a nivel analógico), para el módulo de acondicionamiento y para la adquisición de los datos. En cuarto lugar, en el capítulo 4, describe las características de los *Health Test*, definiendo sus tipos y proponiendo dos pruebas continuas que han sido aprobadas: *Repetition Count Test* y *Adaptive Proportion Test*.

En quinto lugar, en el capítulo 5, define métodos para el análisis de la hipótesis de que la fuente de ruido es IID (*Independent and Identically Distributed*). Las pruebas propuestos son 11 test estadísticos basados en permutaciones y otros 5 basados en la distribución *Chi-square*. Dichas pruebas son distintas a las propuestas en NITS SP 800-22 [8], por lo que se pueden usar como pruebas complementarias.

En sexto lugar, define métodos para la estimación de *min-entropy* producida por ruido muestreado, a lo que da gran importancia para asegurar que se introduce suficiente entropía en la entrada del RGB propuesto en [26].

AIS-31 [32] es otro estándar que define una metodología para la creación de módulos criptográficos. Es analizado y usado por BSI (*Bundesamt für Sicherheit in der Informationstechnik*), la agencia federal alemana responsable de la ciberseguridad, su metodología es considerada como el estándar europeo para evaluar los RNG [33].

Finalmente, es necesario realizar una comparación sobre las baterías de pruebas y estándares citados en esta sección para determinar cuáles son más fiables. En primer lugar, **FIPS 140-2** [21] es identificado por los artículos que tratan el tema como uno de los menos exigentes. A pesar de

ser uno de los estándares más usados por RNG comerciales al permitir una fácil implementación en hardware, se ha conseguido pasar sus pruebas introduciendo secuencias sesgadas de datos de las cuales se conoce su deficiente aleatoriedad [34]. En segundo lugar, **NITS SP 800-22** [8] está formado por una batería de pruebas más complejas y es el más extendido dentro de los artículos sobre diseños de RNG. A pesar de esto, son varios los autores que consideran a **Diehard** [15] más estricto y se suele usar como un complemento a **NITS SP 800-22** para asegurar la aleatoriedad, como en [14] [16] [18]. En tercer lugar, se puede afirmar que **TestU01** [20] es una de las librerías de test más completas de la actualidad. Por último, en cuanto a los estándares **NIST SP 800-90B** [27] y **AIS-31** [32], ambos son ampliamente usados, el primero en Estados Unidos y el segundo en Europa.

2.3. CLASIFICACIÓN DE LOS GENERADORES

Para la generación de números aleatorios existen múltiples métodos cada uno de ellos válido para determinadas aplicaciones. La primera gran división que se puede aplicar al estado del arte de los RNG es entre generadores determinísticos y no determinísticos, conocidos tambien como *Pseudo Random Number Generator* (PRNG) y *True Random Number Generator* (TRNG) respectivamente.

Los **PRNG** generan números aleatorios usando ecuaciones matemáticas capaces de producir a partir de un valor inicial (la semilla) sucesivos valores aparentemente aleatorios. La problemática reside en que al estar generados directamente por una algoritmo, si se conocen los parámetros del algoritmo y la semilla usada, un atacante puede predecir toda la secuencia aleatoria. Debido a esto, se denominan generadores determinísticos ya que su salida no está producida por una fuente aleatoria per se. Si se usan la misma semilla el algoritmo siempre generará la misma secuencia aparentemente aleatoria.

Por otro lado, presentan múltiples ventajas derivadas del hecho de que al ser ecuaciones matemáticas se implementan de forma íntegra en software. Una de ellas es la facilidad con la que se pueden integrar dentro del sistema electrónico donde se necesitan los números aleatorios, al consistir en una serie de cálculos computacionalmente sencillos que se pueden ejecutar dentro del propio sistema. Otra ventaja derivada de la anterior es la eficiencia energética que presentan, pues no necesitan ni de hardware específico para la generación, ni de periféricos para poder integrarlo dentro del sistema. Además, al ser algoritmos poco pesados son capaces de alcanzar una alta tasa

de generación en un breve periodo independientemente de la arquitectura del sistema donde se implemente.

Los **TRNG** usan fenómenos físicos que no se pueden predecir como fuente de entropía para la generación de números aleatorios. Debido a que se necesita traducir los fenómenos físicos a una señal eléctrica de bits aleatorios, los TRNG requieren de hardware específico. Es por esto por lo que son sistemas mucho más costosos tanto a la hora del diseño, como de su fabricación; especialmente, si se requiere un gran número de generadores como puede ser el caso de los sistemas IoT. Para los diseñadores de TRNG supone un reto conseguir sistemas baratos que se puedan embeber fácilmente en los sistemas donde se necesite el cifrado.

Otro de los principales retos es conseguir fuentes de entropía que no dependan de factores determinísticos que un atacante pueda modificar de forma maliciosa para reducir la aleatoriedad del generador. Por ejemplo, si un generador usa únicamente el ruido electromagnético ambiental como fuente de entropía el sistema podría ser atacado si se transmite una señal determinística que afecte a los bits aleatorios generados. Debido a esto diversos autores utilizan una combinación de múltiples fuentes de ruido, como en [35] donde se utiliza un *discret time chaos* combinado con ruido térmico.

Tambien hay que considerar como uno de los retos más notorios la auditabilidad de los generadores, ya que, como se explicó en el apartado *2.2*, existe una gran diversidad de test para medir la aleatoriedad de los circuitos. Además, no es solo el hecho de poder medir la aleatoriedad en la salida, si no poder analizar las etapas intermedias del circuito para analizar su correcto funcionamiento. Con esto último se pueden evitar ataques de *hardware troyan.*

Por último, podemos identificar como otro de los retos el conseguir fuentes de entropía no solo robustas ante interferencias externas, sino que alcancen niveles de aleatoriedad elevados. Debido a que muchas de las fuentes de ruido usadas no consiguen pasar los test estadísticos de aleatoriedad, los desarrolladores usan técnicas de postprocesado que resuelvan el sesgo de la salida de sus fuentes de ruido. Los métodos más usados son **SHA-256** [36] , **XOR-ing** y **Von Neumann method** [37].

Dentro de los TRNG, para capturar los fenómenos físicos existe una gran diversidad de propuestas que se pueden agruparse en tres grandes bloques según la fuente de ruido que usan: basados en *fuentes de ruido directas*, basados en *osciladores* y basados en la *metaestabilidad*.

Los primeros, los basados en *fuentes de ruido directas*, son aquellos que amplifican señales eléctricas procedentes de sensores o del propio ruido generado por componentes electrónicos. Entre los más clásicos se encuentran los basados en ruido térmico [38], efectos cuánticos [39], sensores bio-electromecánicos [40], sensores EEG [41] o diodos de avalancha [42]. Existen aparte de los citados un gran número de propuestas. En general estos RNG presentan múltiples vulnerabilidades, principalmente debido a que muchos de los fenómenos toman entropía de fenómenos físicos externos o se ven influenciados de forma indirecta por estos. También requieren de componentes electrónicos de precisión ya que se necesitan amplificar las fuentes de ruido con una alta ganancia, con un bajo offset a la salida e introduciendo la menor cantidad de ruido externo.

Los segundos, se basan en el fenómeno conocido como *jitter* producido por osciladores. Este fenómeno es el error cometido por los osciladores al presentar pequeñas variaciones no constantes en el periodo de la señal que generan. Los RNG que usan este fenómeno utilizan múltiples osciladores y tras comparar su salida obtienen una señal aleatoria. Algunos ejemplos son [43] o [44].

Los terceros, se basan en el fenómeno de *metaestabilidad*. Dichos generadores están implementados con puertas lógicas y biestables completamente digitales. Para producir la metaestabilidad usan esquemas de conexión atípicos como, por ejemplo, en los que conectan las salidas a las entradas del circuito generando un caos eléctrico que produce una salida aleatoria [45].

Por último, analizando el *Lampert Circuit*, lo podemos clasificar claramente dentro de los TRNG y dentro de estos en los basados en fuentes de ruido directas. El RNG analizado en este estudio utiliza dos diodos de avalancha como fuentes de ruido independientes. Una de las principales ventajas es que el ruido que captura esta generado por un componente interno del circuito y no utiliza fenómenos físicos externos. A pesar de esto no se puede descartar que tanto el fenómeno de la avalancha como el comportamiento del resto de componentes pueda verse influenciado por factores externos.

Otra de las ventajas es que este implementado únicamente con componentes electrónicos discretos que se pueden adquirir fácilmente. Esto lo convierte en un circuito especialmente auditable, económico y accesible, al poderse realizar mediciones intermedias de cada etapa del circuito y poder ser fabricado por cualquier investigador interesado. Esto no sucede para los

generadores embebidos dentro de circuitos integrados, que requieren de un proceso de fabricación más complejo y costoso.

Sin embargo, también presenta inconvenientes frente a los RNG incorporados en un único circuito integrado. Por un lado, presentan en líneas generales un consumo más reducido y un menor tamaño. Por el otro lado, aunque para la fase de diseño e implementación se han mucho más costosos para largas cadenas de producción el coste se reduce.

Se concluye de la comparación del *Lampert Circuit* con el estado del arte de los RNG que se trata de una propuesta innovadora que aporta valor y que presenta cualidades capitales para incorporarse dentro de un entorno IoT.

Capítulo 3. DEFINICIÓN DEL TRABAJO

3.1. METODOLOGÍA

Como se ha expuesto en el punto *1.2*, el principal objetivo es auditar los resultados de las pruebas realizadas en este artículo y complementarlas añadiendo modificaciones y nuevas propuestas. Para replicar los experimentos lo más fielmente posible, a lo largo del proyecto se ha mantenido la máxima de ceñirse a lo especificado en el artículo [1]. En caso de duda sobre lo que el artículo describe, ya sean sobre la implementación del circuito o sobre las pruebas realizadas, se ha consultado directamente con los autores con el objetivo de replicar las condiciones de los experimentos lo más fielmente posible.

El proceso de replicación de las medidas no ha sido sencillo especialmente por la falta de documentación de cómo se realizaron en el artículo [1]. Debido a esto se han acabado realizando múltiples medidas que analizan un mismo aspecto del circuito, pero de las cuales cada una siguen un proceso de aprendizaje respecto a las medidas anteriores. No todas las medidas se han usado para extraer las conclusiones finales del proyecto, en consecuencia, se ha centrado la documentación del proyecto en las medidas finales dentro de cada categoría pero que son fruto de lo aprendido con todas las mediciones anteriores.

La metodología general que se ha llevado a cabo para la toma de cada medida ha sido la siguiente:

1. Configuración del entrono: de la fuente de alimentación, el generador de señales y el osciloscopio y conectarlos al circuito del que se van a realizar las medidas.
2. Conectar el osciloscopio al ordenador con el software de Tektronix**, TekVISA** [46]**.** Este software nos permite leer los datos del osciloscopio desde MATLAB a través de la red LAN del laboratorio.
3. Ejecución de los scripts de MATLAB ***automatizacion_muestreo_*.m*** (*automatizacion_muestreo_diodo.m, automatizacion_muestreo_estandar.m, automatizacion_muestreo_multiples_frec.m*). Estos scripts son los encargados de adquirir las muestras del osciloscopio y almacenarlas en archivos de datos de MATLAB ***.mat***. Cada archivo se guarda con el nombre del circuito al que corresponden los datos

de muestreo que contiene, por ejemplo, *e01.mat* contiene datos del circuito con el código identificativo *e01*.

4. Ejecución de los script de MATLAB ***analisis_*.m*** (*analisis_diezmado.m*, *analisis_diezmado_Fs_multiple.m*, *analisis_diodo.m*, *analisis_frecuencia.m*, *analisis_frecuencia_Fs_multiple.m*), ***procesarSenalesAleatorias.m*** o ***procesarDatos.m*** y las funciones ***procesarBits.m*** y ***procesarBitsMultipleSampleRate.m.***
5. Ejecución si aplica de los script de visualización de los resultados ***plotDatos.m*** o ***plotSenalesAleatorias.m***.
6. Documentación del proceso de medición y los resultados.

3.2. RECURSOS MATERIALES

A continuación, se especifican los conectores e instrumentos que se necesitarán para replicar las mediciones del artículo.

En primer lugar, para realizar este estudio se han fabricado 25 circuitos de 4 fabricantes distintos (*European Circuits* [47], *Micron20* [48], *ShenZhen2U* [49] y *Wurth* [50]), de este modo se pretende tener una muestra significativa que permita evaluar la influencia del fabricante en el rendimiento del circuito. Para llevar un correcto seguimiento de las mediciones de cada circuito se han numerado cada uno con un código identificativo único. El código comienza por la letra: e, *m*, *s* o *w* en función del fabricante ([47], [48], [49] y [50]). A la letra se le ha añadido un número desde 01 hasta 25 (el número total de circuitos de cada fabricante).

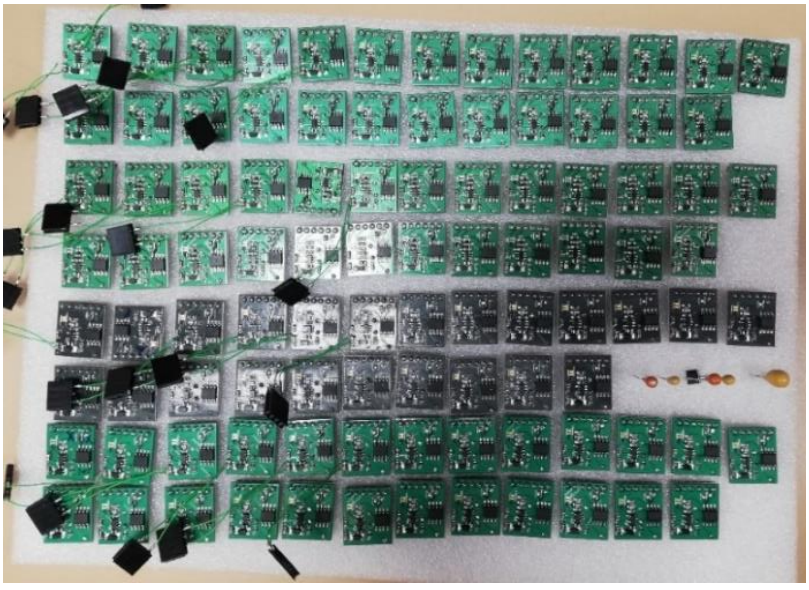


Figura 2: Conjunto de circuitos fabricados para la realización de las pruebas

Con el fin de facilitar y agilizar la toma de medidas se va a elabora un conector hembra, como los clásicos usados en Arduino, al que se le han soldado un cable para cada señal, para poder enganchar todas las sondas del osciloscopio al conector y no directamente al circuito. De esta forma, se consigue agilizar la medición de varios circuitos, ya que no se tienen que estar intercambiando las sondas de un circuito a otro, simplemente se desconecta el conector y se conecta a otro circuito. Un ejemplo de dicho conector se muestra en la Figura 3.

Para determinadas pruebas en las que se necesite estudiar distintos valores de un componente electrónico se va a necesitar soldar un conector mediante unos cables de *wrapping* al circuito impreso. En la Figura 4 se muestra cómo se ha añadido un conector para aumentar la capacidad de un condensador añadiendo otro en paralelo.

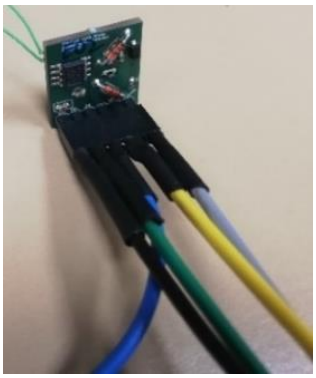


Figura 3: Detalle del conector señales de entrada

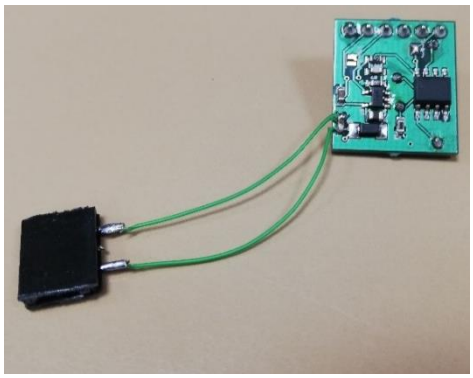


Figura 4: Detalle del conector usado para alargar la curva de descarga

Finalmente, se enumeran los dispositivos de medición avanzados que se van a necesitar. Estos dispositivos se han escogido teniendo en cuenta la precisión y frecuencia de muestreo requeridas para las medidas, así como funcionalidades adicionales como es la extracción de los datos muestreados desde MATLAB.

- Osciloscopio **TDS5104 Tektronix Digital Oscilloscope**: Tiene un ancho de banda máximo de 1GHz, 4 canales y una tasa de muestreo de hasta 5Gs/s [51]. Para exportar los datos del muestreo, el osciloscopio se ha conectado a la red LAN del laboratorio y desde el entorno de programación de MATLAB se han leído los datos.
- Fuente de alimentación **SPD3303C Series Programmable DC Power Supplies** [52] (Figura 6).
- Generador de señales **DG1000Z Series RIGOL Waveform Generators** [53] (Figura 7).

En la Figura 5 se muestra el entorno de trabaja con el ordenador usado para el muestreo, los circuitos y la instrumentación conectada: el osciloscopio (amarillo), el generador de señales (verde) y la fuente de alimentación (azul).

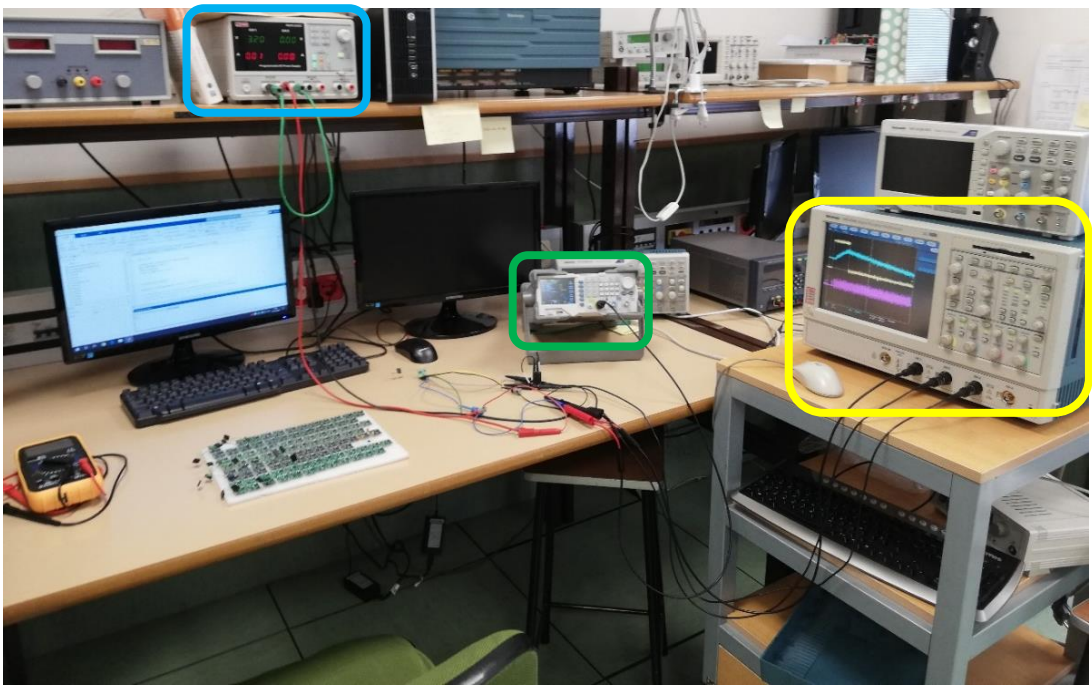


Figura 5: Espacio de trabajo

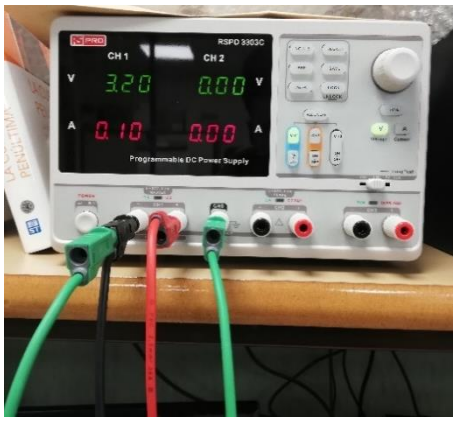


Figura 6: Conexiones de la fuente de alimentación

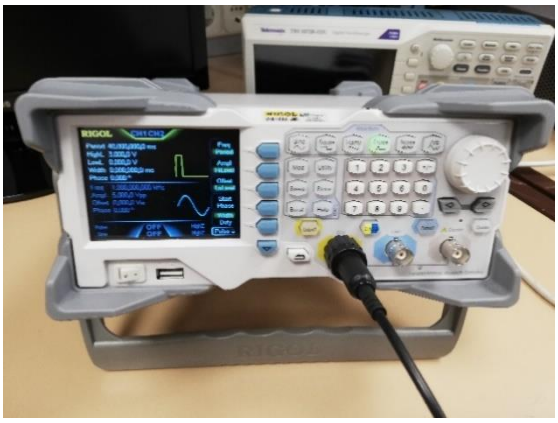


Figura 7: Conexión generador de señales

3.3. PLANIFICACIÓN

En este estudio se va a seguir un esquema clásico de planificación reflejado en la Figura 8. Consta de cinco tareas secuenciales, pero con solapamiento temporal e interrelacionadas (Estado del Arte, Discusión de los Experimentos, Ejecución de los Experimentos, Análisis de Resultados, Extracción de Conclusiones) y una tarea que se realizará en paralelo a todas las anteriores, la "Documentación del Proyecto". Como se acaba de comentar, aunque el flujo de trabajo sea secuencial y una vez acabada una tarea se pase a la siguiente, no se descarta realizar una secuencia cíclica en la que una vez se analicen unas determinadas medidas se vuelva a la etapa de "Discusión de los Experimentos". Este caso se puede dar si en el análisis de las medidas se encuentren deficiencias en los resultados y se decide complementarlas con experimentos nuevos o si se detectan errores en la ejecución de los experimentos.

En primer lugar, se realizará la documentación del Estado del Arte en el que se investigará sobre la importancia que los RNG tienen en la criptografía, sobre el concepto de aleatoriedad y como analizarla, y, por último, sobre los distintos tipos de RNG que existen.

En segundo lugar, se realizará la tarea "Discusión de los Experimentos" en la que se escogerán los métodos de análisis que se van a usar y se estudiará qué instrumentos son necesarios para realizar dichas medidas. En tercer lugar, se realizarán los experimentos y, finalmente, en cuarto y quinto lugar, se analizarán los resultados para posteriormente extraer las conclusiones pertinentes.

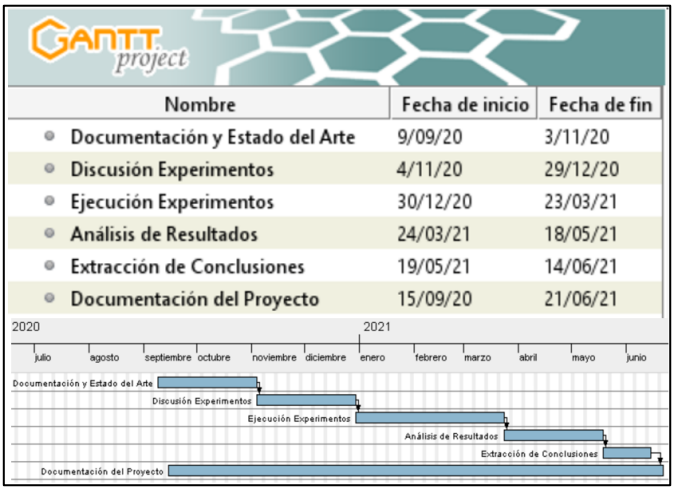


Figura 8:Planificación del proyecto

3.4. ESTIMACIÓN ECONÓMICA

En este apartado se realiza una estimación del coste total de este proyecto teniendo en cuenta tanto el material usado como el coste humano.

3.4.1 COSTE MATERIALES

Los costes materiales del proyecto son los correspondientes con la instrumentación requerida en el punto *3.3 Recursos Materiales*. En primer lugar, hay que indicar que tanto el osciloscopio [51], el generador de señales [52] y la fuente de alimentación [53], requeridos para realizar las medidas se encontraba ya disponible en la universidad, por ello no se han incluido dentro de los costes.

En la Tabla 1 se recoge el coste de los 100 circuitos fabricados divididos por el coste para cada fabricante, así como, el coste del resto de materiales y componentes electrónicos usados en las mediciones.

Tabla 1: Costes Materiales del Proyecto

Coste Material	
PCBs European Circuits	922,26 €
PCBs Micron20	582,20 €
PCBs ShenZhen2U	366,00 €
PCBs Wurth	1.415,70 €
Conectores 2.54mm Hembra Estándar	9,99 €
Condensadores de distintas capacidades	11,70 €
Diodos 1N759A	2,74 €
Resistencias 10K 1% 0.4W	0,90 €
Estaño Soldadura Electrónica	12,10 €
Cable de Wrapping	6,50 €
Coste Material Total:	**3.330,09 €**

3.4.2 COSTE HUMANO

En la Tabla 2 se muestra el coste humano basándose en las horas dedicadas a este estudio. Para cuantificar el coste se han multiplicado las horas dedicadas por un coste medio estimado por hora para un ingeniero de 30€/h.

Tabla 2: Coste Humano del Proyecto

Coste Humano			
Fecha		**Horas**	**Coste (30€/h)**
2020	Julio	45	1.350 €
	Septiembre	15	450 €
	Octubre	21	630 €
	Noviembre	19	570 €
	Diciembre	41	1.230 €
2021	Enero	53	1.590 €
	Febrero	70	2.100 €
	Marzo	31	930 €
	Abril	35	1.050 €
	Mayo	71	2.130 €
	Junio	161	4.830 €
	Julio	95	2.850 €
Coste Humano Total:		463 h	**13.890,00 €**

Finalmente, si se suma el coste material al coste humano se obtiene un coste total del proyecto de **17.220,09 €.**

Capítulo 4. ANÁLISIS TEÓRICO DEL CIRCUITO

En esta sección se ha realizado un análisis detallado del *Lampert Circuit*. No sólo se ha estudiado el diseño teórico del circuito con componentes ideales, sino que también se han explicado los requisitos a la hora de implementar el circuito en una PCB y la elección de los componentes. Para realizar el análisis, el circuito se ha divido en tres bloques: la fuente de alimentación, el generador de ruido y el comparador final.

4.1. ANÁLISIS DE LA FUENTE DE ALIMENTACIÓN

4.1.1 ANÁLISIS DEL DISEÑO TEÓRICO

A la hora de implementar el circuito en un sistema real surge la problemática de que la mayoría de los sistemas empotrados en los que se implementaría funcionan en el rango de 1’8V y 3’3V, mientras que el punto de trabajo del diodo de avalancha está por encima de 12V. Por lo tanto, se necesita una fuente de alimentación que pase de 3’3V a una tensión mayor de 12V. Para realizar esta función los diseñadores escogieron un tipo de circuito denominado *boost converter*, mostrado en la Figura 9.

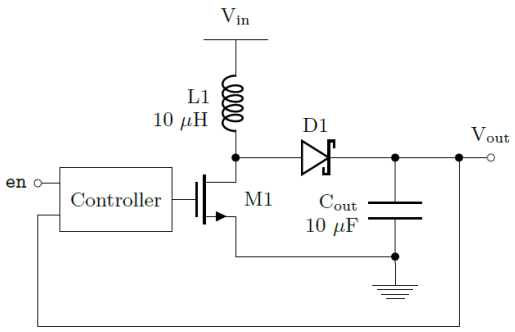


Figura 9: Esquema teórico del boost converter (Fig. 7 de [1])

Basándonos en el esquemático de la Figura 9, vemos que dicho circuito está compuesto por una bobina, un diodo, un condensador y un amplificador MOSFET. El funcionamiento es muy sencillo y consta de varios estados. El primer estado se produce cuando el MOSFET se activa: la corriente circula entre V_{IN} y tierra a través de la bobina, que almacena energía; el condensador queda

completamente aislado. El segundo estado, se produce cuando se desconecta el MOSFET: el diodo conduce y la energía almacenada en la bobina carga hasta la tensión deseada el condensador. Finalmente, cuando se vuelve a activar el MOSFET: el condensador queda aislado y se va descargando, entregando potencia al circuito generador de números aleatorios. El controlador es el encargado de fijar el ciclo de carga o descarga.

El funcionamiento natural de un *boost converter* es, una vez arrancado, mantener la tensión deseada (en nuestro caso 18V) dejando sólo que decremente un pequeño voltaje (conocido como rizado). Esto se consigue con una frecuencia de conmutación del MOSFET elevada, para que el rizado de la salida sea lo menor posible. Sin embargo, los diseñadores identificaron perdidas de entropía en la salida para los puntos en los que el *boost converter* estaba en fase de carga. Por ello, plantean que se controle mediante un *enable* el ciclo de carga y descarga; activando el *enable* para alcanzar los 18V y luego desactivarlo hasta que llegue a los 12V. De este modo se controla la fase de descarga, pudiendo muestrear sólo en esta fase, donde la entropía es mayor.

Por último, hay que indicar que el hecho de que se cargue hasta los 18V, y no hasta los 12-13V que requiere el diodo de avalancha, permite que el margen de descarga hasta alcanzar la tensión mínima de funcionamiento sea mayor y, en consecuencia, conseguir un mayor tiempo de muestreo.

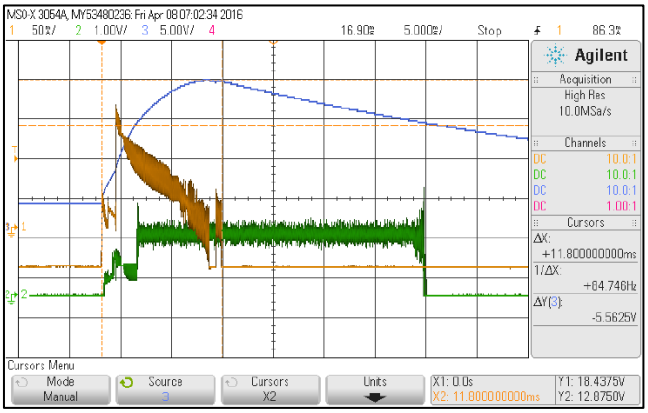


Figura 10: Funcionamiento del boost converter (Fig. 8 de [1])

En la gráfica azul de la Figura 10 se ve como la tensión llega hasta los 18V siguiendo una determinada curvatura, que va seguida de una descarga bastante alargada. También se ve como la corriente de entrada al *boost converter* (grafica amarilla) es inicialmente mayor, decreciendo linealmente hasta que el condensador está completamente cargado.

4.1.2 ANÁLISIS DE LA IMPLEMENTACIÓN

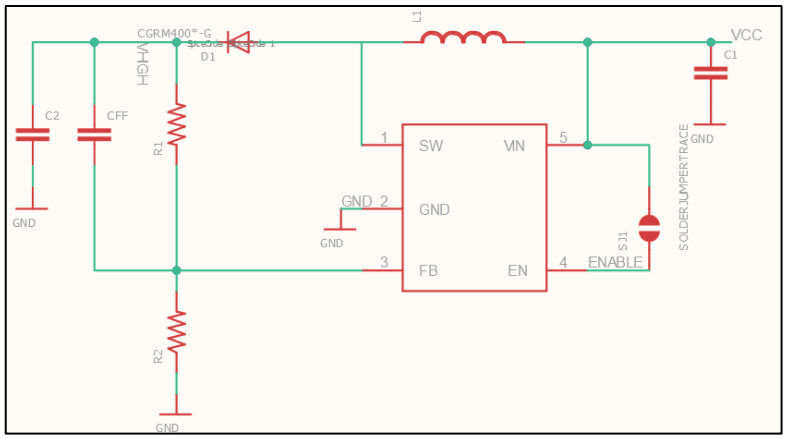


Figura 11: Esquemático de la PCB para el boost converter [54]

Para implementar el *boost converter* los autores han usado como controlador el circuito integrado TPS61041 [55]. Este permite configurar mediante L1, R1, R2 y C_{FF} la frecuencia de carga, la de descarga o la tensión de salida. Para calcular los valores de estos componentes se puede consultar el *datasheet* donde explican cómo realizar el cálculo [55]. Los valores de los componentes utilizados pueden consultarse en la Tabla 3. Esta configuración permite, para una tensión de entrada de entre 1'8V y 6V, alimentar el circuito con 18V y entregar hasta 10mA de corriente.

Tabla 3: Componentes de configuración del controlador según la datasheet [55]

Componentes Boost Converter	
R1	2.2MΩ
R2	160kΩ
D1	MBR0530
C1	10µF
C2	470nF
C_{FF1}	22pF

Por otro lado, al realizarse las primeras mediciones del circuito, uno de los puntos que no concuerdan con lo descrito en el artículo sobre el *boost converter* (Figura 10) es la forma en la que se carga el condensador. Al medir la señal de V_{HIGH} en el laboratorio se observó que no seguía una curvatura constante (como si lo hace en la gráfica adjunta en el artículo Figura 10), sino que parecía cargarse en 2 etapas (Figura 13).

Sin embargo, la curva de carga medida sí coincide con la gráfica de arranque de la *datasheet* del controlador del *boost converter* (Figura 12). En el apartado 7.3.2 de la *datasheet* [55] se explica que,

debido al funcionamiento del *chip*, en el arranque alcanza corrientes elevadas si no se limita y puede llegar a dañarse. Esto puede causar caídas de voltaje en el sistema donde se implemente el *Lampert Circuit* e incluso el apagado. Para conseguirlo, limita primero a $I_{max}/4$, después a $I_{max}/2$ y, finalmente, permite hasta I_{max}.

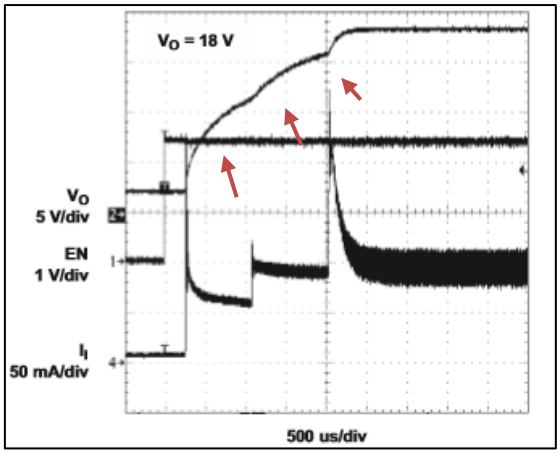


Figura 12: Gráfica de carga del boost converter para Vo=18V (Fig. 15 de [55])

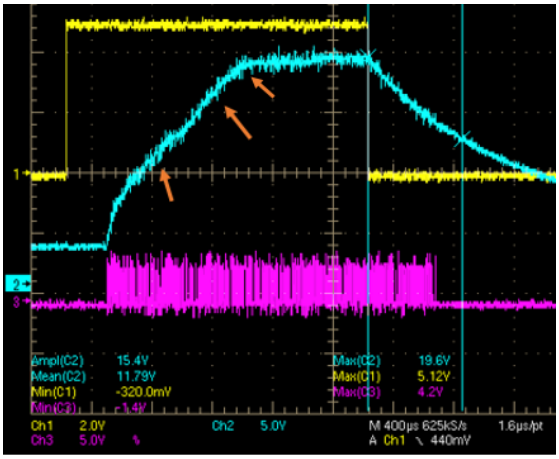


Figura 13: Medición de un ciclo de muestreo. Se ha capturado la señal enable (amarillo), la salida del boost converter (azul) y la salida aleatoria

Por último, al comparar el diseño planteado en el artículo (Figura 9) y el que usaron en la implementación de la PCB (Figura 11) se ha llegado a la conclusión de que son distintos. Aunque el funcionamiento es similar y se hayan usado los mismos parámetros de diseño, el *boost converter* de la PCB tiene un funcionamiento más complejo que el documentado en el artículo. La primera diferencia es el funcionamiento del *boost converter* en el arranque, explicado anteriormente. La segunda, la duración de la descarga al desactivar el *enable* y esperar a que pase de los 18V hasta el fin de la generación de números aleatorio. En el diseño descrito en el artículo la fase de descarga dura hasta los 20 ms, mientras que en las mediciones realizadas sobre las PCB salió un tiempo medio de descarga de 0,525 ms. Esta diferencia en los tiempos es tan grande que se plantea si la implementación del *Lampert Circuit* de las PCB probadas estaba hecha para funcionar con el *enable* siempre activo. El desarrollo de estas medidas se describe en detalle en el apartado 7.1.: *Medidas de la Fase de Descarga.*

Hay que puntualizar que dichas discrepancias no son derivadas de que se haya fabricado un circuito distinto al usado para las pruebas del artículo, sino que posiblemente en el artículo usaron un *boost converter* distinto para el diseño inicial. La justificación de que se ha usado exactamente el

mismo circuito al diseñado en el artículo se explica más adelante en el *Capítulo 6: Fabricación de los Circuitos*.

4.2. ANÁLISIS DEL GENERADOR DE RUIDO

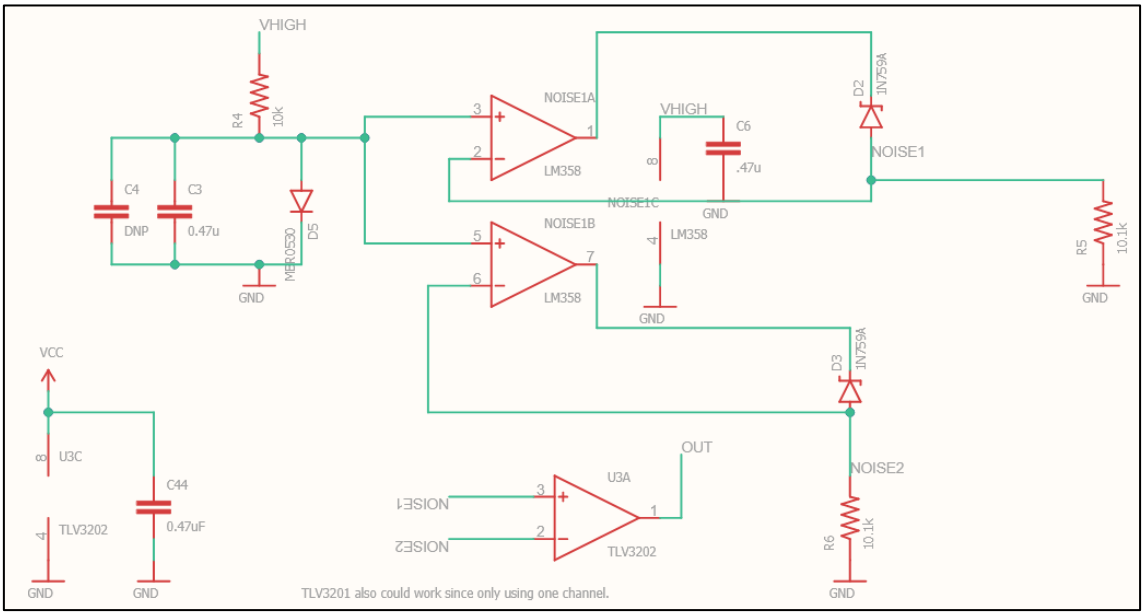


Figura 14:Esquemático de la PCB para los dos Generadores de Ruido [54]

El bloque del generador de ruido está compuesto por una primera etapa en la que se fija la tensión de referencia y una segunda, en la que se usa la realimentación negativa para generar de forma constante la señal aleatoria.

4.2.1 PRIMERA ETAPA

La primera etapa, usando la nomenclatura de la Figura 14:Esquemático de la PCB para los dos Generadores de Ruido , está compuesta por la resistencia R4, los condensadores C4 y C3 y el diodo D5. La funcionalidad del diodo D5 junto con la resistencia R4 es fijar la tensión de referencia (V_{REF}) necesaria para el generador de ruido. El componente D5 (MBR0530) es un diodo *Schottky* con una tensión de *forward* típica de 0,337V [56]. Se trata de un diodo capaz de proporciona conmutaciones a gran rapidez entre el estado de conducción directa y el de conducción inversa. Además, dicha conducción inversa se produce a tensiones muy bajas. Pero la cualidad que nos interesa es que la tensión que cae en estado de *forward* es baja.

Variaciones en V_{REF}

Sabemos gracias a las medidas realizadas en el laboratorio que V_{REF} tiene un valor medio de 184mV (documentadas en *6.2.3 Medición de las Fuentes del Ruido con Realimentación*). Con este valor podemos calcular la corriente que pasa por el diodo con la siguiente ecuación:

$$V_{HIGH} - V_{DIODO} = R_4 * i_{DIODO}$$

Para el caso de la tensión máxima a la salida del boost converter (V_{HIGH} = 18V), obtenemos una corriente de 1,781mA:

$$18V - 184mV = 10k\Omega * i_{DIODO\ MAX}$$

Esta corriente no será constante ya que la ecuación depende de V_{HIGH} y, esta tensión, como se ha explicado en el punto *2.1 Análisis de la Fuente de Alimentación*, pasa de los 18V hasta los 12V-13V. Además, como la corriente que pasa por el diodo está relacionada directamente con la tensión que cae en el diodo (Figura 7) está también cambiará. Para estimar el cambio se ha considerado en primer lugar que la V_{REF} es fija y se ha calculado que la corriente mínima será de 1,182mA:

$$12V - 184mV = 10k\Omega * i_{DIODO\ MIN}$$

Según la Figura 15, para la temperatura típica de funcionamiento de 25ºC, un cambio en la corriente de 0.599mA (1,781mA menos 1,182mA) va a ser menor que 5mV aproximadamente, por lo que podremos despreciar dicha variación en V_{REF}. Dicha variación menor que 5mV se ha podido confirmar experimentalmente en las medidas documentadas en el punto *6.2.3*.

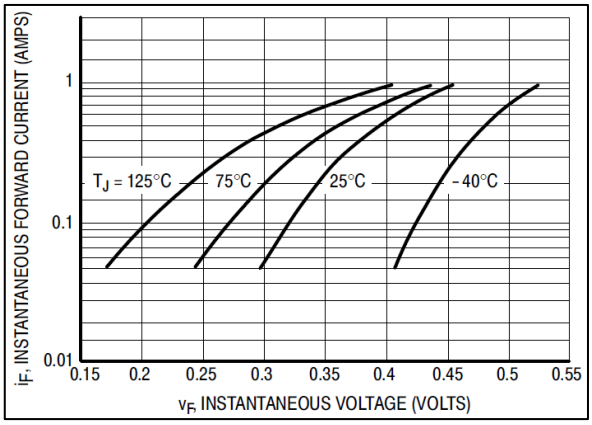


Figura 15: Typical Forward Voltage (Fig. 1 de [56])

Propagación de Ruido no deseado

En cuanto a la finalidad de C4 y C3, sabemos que se trata de dos condensadores que están conectados entre V_{REF} y GND. La finalidad es actuar a modo de filtro paso bajo eliminando las frecuencias altas. La utilidad de estos condensadores es crucial para que no se propague el ruido generado en la fuente de ruido al resto del circuito.

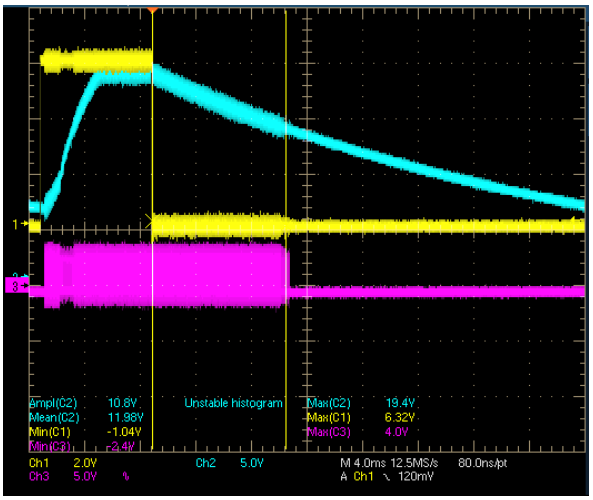


Figura 16: Medición de un ciclo de muestreo con 12,5MHz. Se ha capturado la señal enable (amarillo), la salida boost converter (azul) y la salida aleatoria (magenta).

Se considera que sería conveniente aumentar esta capacidad para reducir el ruido inducido en V_{HIGH} y la señal de *enable*. En la Figura 16 se ve claramente como en los instantes en los que se está generando una salida aleatoria, el ruido de la señal V_{HIGH} y *enable* es claramente superior que en los momentos en los que no se está generando una señal aleatoria. Se podría justificar que se está acoplando el ruido en las sondas del osciloscopio usado para tomar las medidas, pero se ha probado al desconectar la sonda conectada a la salida aleatoria del circuito y el ruido medido en las otras dos señales sigue siendo el mismo; es decir, se está acoplando dentro del propio circuito.

4.2.2 SEGUNDA ETAPA

En esta etapa se han usado dos fuentes de ruido distintas, cada una con su bucle de realimentación. El diodo usado para para la generación de ruido es el *Zener* 1N759A [57], que tiene una tensión Zener nominal (V_{ZENER}) de 12V con una tolerancia del 5%.

Los diodos Zener en sentido directo se comportan como un cortocircuito, en el caso ideal, y con una muy pequeña resistencia en el real. Sin embargo, en sentido inverso son capaces de conducir cuando la tensión en sus extremos alcanza el valor de la V_{ZENER}. Al proceso de cambio de estado entre no conducción y conducción en sentido inverso se le conoce como *reverse breakdown.*

El *reverse breakdown* es el resultado de las colisiones entre electrones dentro de la red cristalina de un material semiconductor. Como se explica en el artículo [1], cada electrón dentro del semiconductor se encuentra asociado a varias bandas de valencias (con distintos niveles de energía cada una). Los electrones pertenecientes a la red cristalina se encuentran fuertemente unidos al átomo y, en consecuencia, esta red no conduce la electricidad. Sin embargo, existen electrones energéticos que se encuentran débilmente unidos a la red cristalina y que si son capaces de conducir; a esta franja se le conoce como banda de conducción.

En condiciones normales el número de electrones que pertenecen a esta banda es bajo y la corriente existente es muy baja. A pesar de esto, si el campo eléctrico que atraviesa la red cristalina aumenta, los electrones de la banda de conducción se empiezan a acelerar. Cuando estos electrones empiezan a impactar con los electrones que no se encuentran en la banda de conducción, les transfieren la energía cinética que han alcanzado y los arrastran a la banda de conducción.

La propiedad que nos interesa es que se trata de un proceso completamente aleatorio, ya que tanto la frecuencia de colisiones que se producen como la intensidad con que lo hacen no se puede predecir. Debido a esto, en el proceso de *reverse breakdown* se produce una corriente de avalancha de carácter aleatorio y que se usa como fuente de ruido.

Análisis del diodo Zener

En primer lugar, se ha analizado la datasheet del componente [57]. Se ha conocido que se trata de un diodo con una V_{ZENER} media 12V y cuyos máximos y mínimos son 12,60 y 11,40V respectivamente. Además, se especifica que su resistencia Zener máxima (R_{Z_MAX}) es de 30Ω y la corriente *Reverse Leakage* máxima que es de 0,1μA para una tensión de 1V.

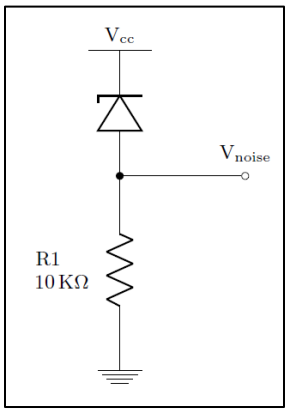


Figura 17: Esquema de conexión para medir el ruido del diodo (Fig. 2 de [1])

En segundo lugar, se ha querido contrastar la información de la datasheet con el comportamiento del diodo tal y como se muestra en el apartado 3.1 del artículo [1]. En este apartado se analizan distintas fuentes de ruido para un RNG y explican porque el diodo de avalancha es una buena opción. Para probarlo en el artículo se usó el esquema de la Figura 17 y se midió la tensión en V_{NOISE} tomando 500000 muestras con un periodo de muestreo de 1ns. El resultado obtenido fue el de un ruido medio de 160mV con una desviación de la media de ±60mV (Figura 18 y Figura 19).

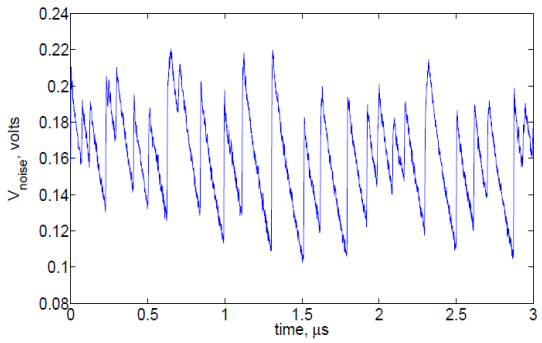


Figura 18: Amplitud del ruido en el dominio del tiempo (Fig. 3 de [1])

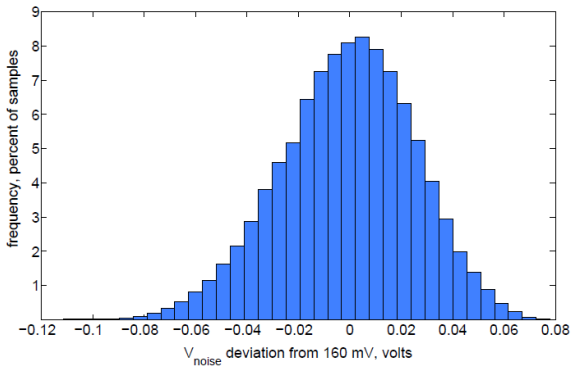


Figura 19: Desviación del nivel medio del ruido (Fig. 4 de [1])

Esta prueba hace dos suposiciones simplificadoras. Primero, asume que la tensión de alimentación requerida, V_{CC}, está fija. En la práctica, el punto de funcionamiento del circuito cambiará con el tiempo, la temperatura y otros factores. Por lo que en otro momento, el circuito puede necesitar un valor diferente de V_{CC} para establecer el punto de funcionamiento deseado. En segundo lugar, la prueba asume que no hay perturbaciones externas en el sistema que afecten al ruido, como puede ser el ruido generado por la propia fuente de alimentación.

Debido a que en el datasheet [57], elaborado por el fabricante del diodo, no contiene información suficiente respecto al comportamiento del diodo (especialmente sobre el ruido que puede llegar a general) se ha creído conveniente hacer nuestras propias medidas experimentales. Dichas medidas se describen en el apartado *6.2 Medidas de la Fuente de Ruido* de esta memoria.

Bucle de realimentación

El punto óptimo de la generación ruido se puede hacer ajustando la tensión V_{ZENER} para que se encuentre constantemente en el estado de *reverse breakdown*, pero esto requiere una fuente de alimentación muy precisa y estable en el tiempo.

La solución propuesta en el artículo es la implementación del control del nivel medio mediante una realimentación negativa. El circuito utiliza realimentación negativa para establecer el valor promedio del ruido con un amplificador operacional, como se muestra en Figura 14. En esta configuración, la función del amplificador operacional es hacer que el valor medio de V_{NOISE} sea igual al valor de V_{REF}. El resultado es que el circuito consigue corregir las diferencias de fabricación entre los diodos de avalancha, las variaciones debido a factores externos como la temperatura, el envejecimiento o la variación de V_{CC}.

El funcionamiento es el siguiente: Si partimos del estado inicial del circuito apagado y lo encendemos, V_{HIGH} va incrementando progresivamente a medida que el *boost converter* se va cargando. En la Figura 20 se muestra el arranque del circuito, con una duración de 4’6ms hasta que V_{HIGH} alcanza V_{ZENER}. En esta fase la tensión en a la salida del operacional (polo negativo del diodo) es menor que V_{ZENER} y el diodo no conduce (solo se escapa una pequeña corriente *Reverse Leakage* de pocos µA [57] despreciable para el orden de magnitud con el que estamos trabajando). Como esta corriente es aproximadamente 0mA, podemos afirmar que en la resistencia de 10kΩ en serie al diodo no cae tensión; por lo tanto, V_{NOISE} y la tensión en el input negativo del operacional es aproximadamente 0mV. Siguiendo el bucle, si la tensión en el input negativo del operacional es de

0mV al compararse con V_{REF} (input positivo del operacional), que tiene un valor 128±5mV, el operacional saturará positivamente (hasta alcanzar una tensión aproximadamente mayor que V_{ZENER}) al existir una diferencia positiva de tensión en la entrada. Volviendo otra vez al polo negativo del diodo ahora la tensión existente es mayor que V_{ZENER} y en este caso la tensión si es lo suficientemente grande para que se produzca la avalancha, lo que provoca que la *reverse current* del diodo incremente drásticamente. Dicha corriente circulará por la resistencia de 10KΩ, ya que es mucho menor que la resistencia de entrada del input negativo del operacional. Esta corriente provoca un aumento en la tensión V_{NOISE} (que es la misma que la de la entrada del input negativo). Volviendo otra vez a la entrada del operacional, sabemos que la corriente seguirá creciendo hasta que la tensión en el input negativo supere a V_{REF}, momento en el que la salida del operacional pasará a saturar negativamente cayendo la tensión en la salida. La tensión no baja excesivamente de los 12V, aunque estando por debajo de V_{ZENER}. De este modo se vuelve a tener 0V en el polo negativo del diodo, repitiéndose de nuevo el mismo proceso. El funcionamiento nominal del circuito se muestra en la Figura 21. En la Figura 20 se puede ver como V_{HIGH} debe ser siempre mayor que V_{ZENER}, de lo contrario el diodo no alcanzará la tensión de breakdown y dejará de estar en estado constante de generación de ruido.

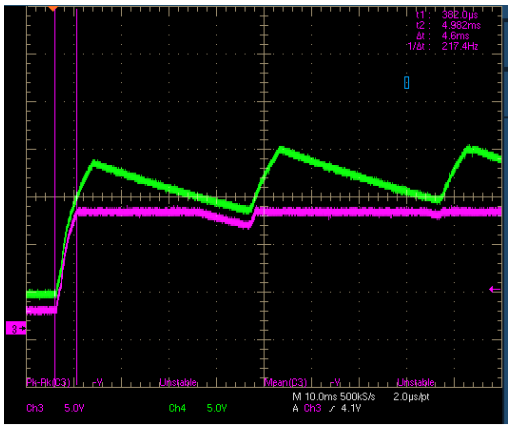


Figura 20: Arranque del circuito representado con V_{HIGH} (verde) y V_{ZENER} (morado)

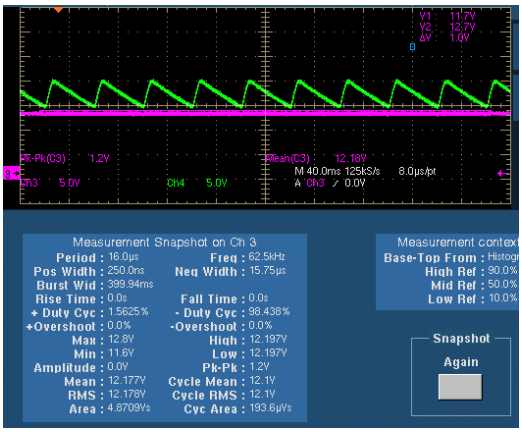


Figura 21: Estado nominal del circuito representado con V_{HIGH} (verde) y V_{ZENER} (morado)

4.3. ANÁLISIS DEL COMPARADOR FINAL

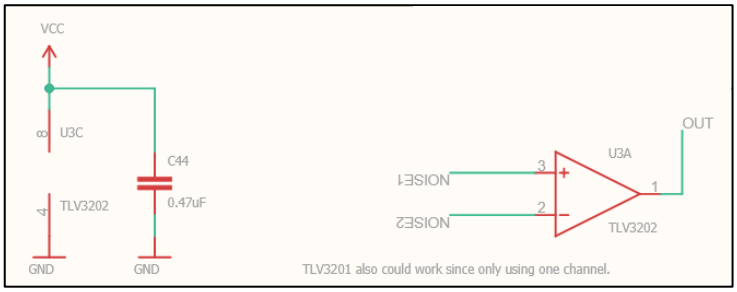


Figura 22: Esquemático de la PCB para el comparador final [54]

Esta última etapa se implementó con un operacional de alta ganancia y bajo consumo, en concreto el TLV3203 [58]. El objetivo de esta última etapa es juntar las dos fuentes de ruido en una única salida completamente aleatoria Figura 22.

En primer lugar, se usa un diferencial y no un sumador, porque también se busca eliminar las variaciones de la fuente de alimentación restado los niveles medios de cada fuente de ruido. Como las dos fuentes de ruido tienen el mismo nivel medio, ya que ambas usan la misma V_{REF}, cuando en el diferencial se restan, el nivel medio se anula.

En segundo lugar, el hecho de que se anule el nivel medio de las fuentes de ruido no implica que el nivel medio de la salida sea de 0V. Dicho nivel medio depende de la alimentación del operacional. En este caso se alimenta a 3’3V y 0V. Por ello el operacional debe saturar a 3’3V o a 0V, por lo que el nivel medio de la salida tendrá que ser idealmente de 1’65V. Si se producen diferencias entre los niveles medios de *NOISE1* y *NOISE2*, el nivel medio de la salida dejará de ser 1’65V y se producirán incrementos y decrementos sobre 1’65V.

Capítulo 5. FABRICACIÓN DE LOS CIRCUITOS

Antes de encargar la fabricación del circuito e iniciar la recreación de los experimentos, se identificaron discrepancias entre los componentes indicados en el artículo publicado en SenSys'16 [1] y el diseño disponible en el GitHub [54] indicado en el artículo. Para resolver las dudas sobre el diseño y fabricar exactamente el mismo circuito con que se hizo el estudio, nos pusimos en contacto con los autores del artículo Ben Lampert y Philip Levis. El intercambio de correos finalizo con una serie de especificaciones acerca del diseño del circuito usado para el artículo que se adjunta a continuación.

---------- Forwarded message ---------
From: ***bn lm*** *<lampert.b@gmail.com>*
Date: Mon, 23 Sep 2019 at 07:18
Subject: Re: Lampert circuit
To: Gregorio López <gllopez@comillas.edu>
Cc: Philip Levis <pal@cs.stanford.edu>, Carlos Rodríguez-Morcillo García <Carlos.Rodriguez@iit.comillas.edu>, Javier Matanza Domingo <jmatanza@icai.comillas.edu>, Julio Hernandez-Castro <J.C.Hernandez-Castro@kent.ac.uk>

Hi Grego,

Please see updated github files:

https://github.com/*lampert*b/*Lampert*CircuitRNG

The Imix files are where the design ultimately converged on, there were a few changes that are now reflected in the design I've pushed:

-Added 1N759A zener diodes to the design which is actually what we tested with I just didn't have the right footprint on the board at the time

-Removed the buffered output (originally thought it would be needed but that turned out to not be the case)

Testing was done by:

1) Powering board with 3.3V supply

2) Enable the TPS boost pin (you can verify the VHIGH/boost output voltage to see when it's fully stabilized)

3) Disable the TPS pin

4) Collect bits from the output PIN (via oscope for high freq correlation testing and MCU for application)

5) Monitor the VHIGH pin until the voltage drops below the Zener diode breakdown voltage (at which point the zener won't have any breakdown occurring and the bit's should not be measured).

6) Repeat to collect more bits

Some notes:

-Feedback makes this circuit fairly robust to component variance, the only critical pieces I would suggest is using 1% resistors on R5/R6 and the 1N759A zener diodes since you are trying to create similar conditions on the input of the op amp

-You can move to the TLV3201 since you only need one output, that op-amp was selected primarily because it can drive pins and respond quickly to the mV deltas on the input from the avalanche noise. Goal is to have a very sensitive high gain op amp that doesn't present much load on the "Noise" nodes.

-D5 is really just there to provide a constant diode drop reference; it's important, but other diodes should work

-TPS boost circuit came from the TI documentation equations if you need to debug it. Nothing too special about the components (this is the L used)

Hope this helps, sorry for the delay it's been a few years since this work so had to context switch back and pull up what material I had.

Thanks,

Ben

Finalmente, debido a que en el GitHub [54] existían dos esquemáticos distintos (la versión antigua y la que especifican en el correo que habían actualizado) nos hemos de asegurar que se ha fabricado el circuito con las especificaciones indicadas en los correos intercambiados. A continuación, se adjunta tanto el esquemático fabricado, como los archivos *gerber* y los componentes usados.

Además, se realizan una serie de comparaciones que justifican que el diseño escogido se adapta a las especificaciones descritas en el correo adjunto.

5.1. ESQUEMÁTICO

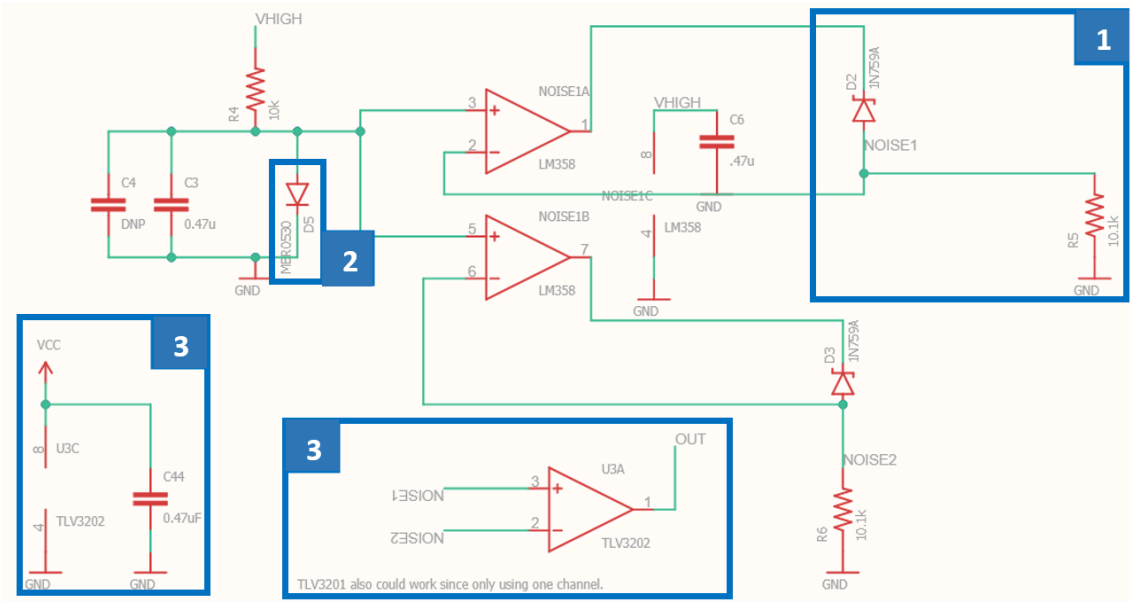


Figura 8: Esquemático Lampert Circuit con referencias [54]

En la referencia 1 en la Figura 8 podemos identificar como se ha usado el diodo 1N759A [57] para la generación de ruido junto con una resistencia de 10kHz con una tolerancia del 1% (10.1k), como se especifica en el correo en la primera anotación y en las indicaciones iniciales sobre los cambios en el GitHub.

En cuanto a la referencia 2, se identifica el uso del diodo D5, MBR0530 [56], para fijar la tensión en el polo positivo del operacional, como se especifica en el correo en la tercera anotación.

En cuanto a la referencia 3, se ha identificado la eliminación del buffer que aparece en otras versiones del circuito y que, como se indica en el correo en la anotación segunda, no es necesario. Aunque se ha usado el operacional TLV3202 [58], con un encapsulado de 8 pines y dos operacionales. Como solo se usa 1, el operacional que corresponde a los pines 5,6,7 se han dejado sin conectar.

Finalmente, hay que indicar que el *TPS boost circuit* corresponde con el de la documentación de la datasheet [55], como se indica en el correo.

5.2. COMPONENTES

La Tabla 4 muestra los datos del archivo BOM (*Bill Of Material*) con los que se han fabricado los circuitos. Dicho archivo BOM se ha extraído de la versión actualizada del GitHub [54], como se especificó en el correo.

Tabla 4: Componentes usados para la implementación de [41]

Reference	Description	Footprint	Fit	Manufacturer	Manufacturer PN	Layer	Technology	Quantity
R4	10k	RNG_Board:0603-RES	Y	TE Connectivity	CRGP0603F10K	Top	smd	1
R5	10k1±1%	RNG_Board:0603-RES	Y	KOA Speer	RN73H1JTTD1012D100	Bottom	smd	1
R6	10k1±1%	RNG_Board:0603-RES	Y	KOA Speer	RN73H1JTTD1012D100	Top	smd	1
L1	10u	RNG_Board:0805	Y	Taiyo Yuden	LBR2012T100K	Bottom	smd	1
C1	10u	RNG_Board:0603-CAP	Y	Murata Electronics	GRM188R61E106KA73J	Bottom	smd	1
R2	160k	RNG_Board:0603-RES	Y	Panasonic	ERJ-3EKF1603V	Bottom	smd	1
D2, D3	1N759A	RNG_Board:DIODE-ZENER	Y	Central Semiconductor	1N759A TR	Top	tht	2
CFF1	22p	RNG_Board:0603-CAP	Y	Würth Elektronik	885 012 006 053	Bottom	smd	1
R1	2M2	RNG_Board:0603-RES	Y	Panasonic	ERJ-3EKF2204V	Bottom	smd	1
C2	470n	RNG_Board:0603-CAP	Y	Taiyo Yuden	UMK107B7474KA-TR	Bottom	smd	1
C3, C6	470n	RNG_Board:0603-CAP	Y	Taiyo Yuden	UMK107B7474KA-TR	Top	smd	2
C44	470n	RNG_Board:C0603	Y	Taiyo Yuden	UMK107B7474KA-TR	Top	smd	1
NOISE1	LM358	RNG_Board:SO8	Y	Texas Instruments	LM358ADR	Bottom	smd	1
J1	M06SILK_FEMALE_PTH	RNG_Board:1X06	Y	Würth Elektronic	613 006 111 21	Top	tht	1
D1	MBR0530	RNG_Board:SOD-123_MINI-SMA	Y	On Semiconductor	MBR0530	Bottom	smd	1
D5	MBR0530	RNG_Board:SOD-123	Y	On Semiconductor	MBR0530	Top	smd	1
U3	TLV3202	RNG_Board:SO8	Y	Texas Instruments	TLV3202AIDR	Top	smd	1
U$1	TPS61041	RNG_Board:SOT23-5	Y	Texas Instruments	TPS61041DBVR	Bottom	smd	1

5.3. GERBER

En la *Figura 23: Esquemas de fabricación de la PCB* se muestran cuatro vistas distintas de los archivos de fabricación en formato *gerber* descargados del repositorio de GitHub [54]. En orden, de izquierda a derecha y de arriba abajo tenemos:

- Vista superior (donde están los conectores) de la PCB. Esta vista representa la PCB tal cual se ve una vez fabricada sin los componentes soldados.
- Vista inferior, que representa al igual que la anterior, la imagen real de la placa.
- Vista superior del plano de cobre, con las huellas de todos los componentes y su correspondiente identificador asociado al archivo BOM de componentes y al esquemático.
- Vista inferior del plano de cobre, con las huellas e identificadores.

Por último, hay que indicar que el pin 4 (empezando a contar por el de GND en la primera vista) corresponde a dónde estaría la salida del buffer que, como se indica en el correo, se eliminó porque no era necesario.

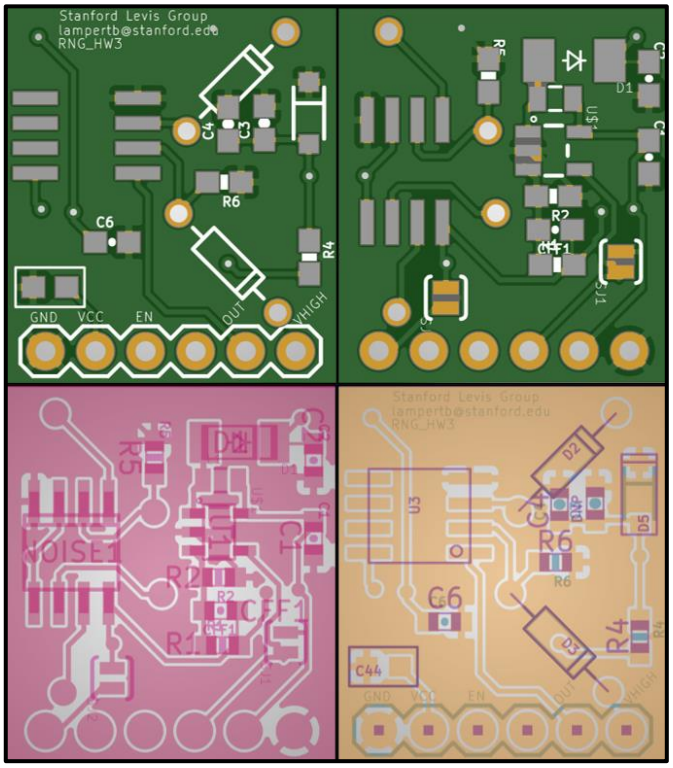


Figura 23: Esquemas de fabricación de la PCB [54]

Capítulo 6. ANÁLISIS EMPÍRICO DEL CIRCUITO

6.1. MEDIDAS DE LA FASE DE DESCARGA

En esta sección se pretende arrojar luz sobre las discrepancias, descritas en el apartado 5.1.: *Análisis de la Fuente de Alimentación*, entre el diseño documentado en el artículo [1] y el realizado en la implementación disponible en [54].

La forma en la que se ha realizado el muestreo es el explicado en [1] :

1. Activar el *enable* hasta que se alcancen los 18V. Aunque en esta fase, desde que alcanza los 12V aproximadamente ya empieza a generar números aleatorios, en el artículo se especifica que no usaron la señal aleatoria de este tramo porque tenía una entropía menor.
2. Una vez cargado el condensador se desactiva el *enable* (a 0V) y se inicia el muestreo. La duración de esta descarga tiene que ser aproximadamente de 12ms.

6.1.1 MEDICIÓN TIEMPO HASTA ALCANZAR LOS 12V

Metodología

Para probar el ciclo de carga y descarga del boost converter se han realizado mediciones sobre 5 circuitos de cada fabricante (20 en total). Se ha usado el osciloscopio TDS5104 [51] tomando 25000 muestras para cada circuito.

Para monitorizar el circuito se han usado tres sondas, la primera (CH1) conectada a la señal de *enable*, la segunda (CH2) conectada a V_{HIGH} (salida del boost converter) y la tercera (CH3) conectada a la salida de números aleatorios. Del osciloscopio se han exportado: los datos de muestreo de la señal aleatoria (en un archivo CSV) y una imagen de las tres señales medidas en tiempo.

El control del *enable* se ha realizado con una señal cuadrada de 3V en *high* y 0V en *low*. La señal tiene un periodo de 6ms y el estado de *high* dura 2ms, tiempo suficiente para que se cargue al máximo el condensador. El circuito se ha alimentado con 3’3V±0’1V. Dichas configuraciones se pueden ver en la Figura 24.

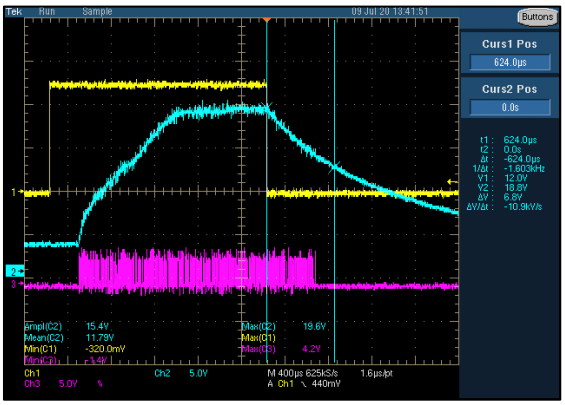


Figura 24: Medición de un ciclo de muestreo. Señal enable (amarillo), salida del boost converter (azul) y salida aleatoria (magenta).

Resultados

Todos los circuitos se han podido medir sin problemas a excepción del circuito m05 (el número 5 de los fabricados por Micron20) y el s02 que no funcionan debido a un cortocircuito entre alimentación y tierra. La Tabla 5 muestra los resultados obtenidos.

Tabla 5: Tiempo de descarga hasta alcanzar los 12V

Tiempo de descarga desde la desactivación del *enable* hasta alcanzar los 12V (ms)						
Fabricante \ ID circuito	**01**	**02**	**03**	**04**	**05**	**Tiempo medio**
ShenZhen2U	1,68[1]	1,71	1,70	1,76	1,56	1,68
European Circuits	0,624	0,752	0,760	0,768	0,656	0,712
Wurth	0,680	0,602	0,723	0,776	0,816	0,719
Micron20	0,812	0,640	0,616	0,784	0,624[2]	0,695

Analizando el tiempo medio de descarga medido para los circuitos de cada fabricante se observa que no hay diferencias significativas, salvo para el caso de los circuitos del fabricante ShenZhen2U. Se observa que para European Circuits, Wurth y Micron20 varía entre los 0'6 y 0'8 ms.

Como no se han identificado discrepancias significativas entre los circuitos fabricados por una misma empresa y entre los de distintas empresas, nos planteamos si es un problema de cálculo de las capacidades que afectan a la descarga o de la corriente que se consume en el circuito. En la práctica no nos interesa cuánto tarda en alcanzar los 12V, sino cuándo deja de producir números aleatorios.

[1] El circuito 01 de Shenzhen2U no funcionan por lo que se han muestreado del 02 al 06.
[2] El circuito 05 de Micron20 tampoco funciona correctamente se ha muestreado el 06 en su lugar.

En el artículo indican que es hasta los 12V, pero por lo que se ha observado en las mediciones es antes. Por ejemplo, en la captura mostrada en la Figura 24 el primer cursor marca el inicio de la descarga y el segundo la llegada a los 12V; sin embargo, la señal morada (la salida aleatoria del circuito) termina de dar números aleatorios mucho antes.

6.1.2 MEDICIÓN TIEMPO HASTA EL FIN DE ALEATORIEDAD

Metodología

Tras analizar las medidas del tiempo de descarga, se decide calcular el tiempo desde que se desactiva el *enable* hasta que el circuito deja de producir números aleatorios. Para ello se usarán los mismos archivos CSV y capturas que se tomaron para el apartado anterior. Como es poco preciso medir en la imagen el tiempo en el que termina la generación de números aleatorios, se utilizaron los archivos CSV. En éstos, está almacenada una medida de voltaje asociada a un tiempo determinado, siendo 0s el momento en el que se desactiva el *enable*, ya que se ha configurado el osciloscopio (el *trigger*) para que capture las señales en el flanco de bajada del *enable*.

Resultados

Los resultados obtenidos se muestran en la Tabla 6:

Tabla 6: Tiempo de descarga hasta el fin de la generación de la salida aleatoria

Tiempo de descarga desde la desactivación del enable hasta el fin de los números aleatorios (ms)						
ID circuito/ Fabricante	**01**	**02**	**03**	**04**	**05**	**Tiempo medio**
Shenzhen2U	1,16	1,28	1,20	1,26	1,27	1,23
European Circuits	0,4992	0,5344	0,5824	0,5696	0,5536	0,5478
Wurth	0,4672	_[3]	0,5680	0,5296	0,6000	0,5412
Micron20	0,5744	0,4336	0,4208	0,5104	0,4312	0,4741

Observamos como el tiempo medio de cada fabricante es aproximadamente el mismo (quitando el valor atípico de los de Shenzhen2U), siendo la media de 0,525 ms. Además, no se identifican variaciones relevantes entre los circuitos de cada fabricante. Sin embargo, a la hora de automatizar las mediciones habrá que tomar la duración mínima medida, 0’4ms, para asegurarnos de medir solo números aleatorios. En 0’4ms si usamos como referencia la frecuencia de muestreo recomendada en

[3] En este caso los números no son para nada aleatorios, en la franja en la que le corresponde a la salida ser aleatoria la señal se encuentra siempre a nivel bajo.

el artículo (128kHZ) tendremos 51 bits aleatorios. Este valor está muy lejos de los 500-800 bits que se deben tomar en cada ciclo de muestreo, por lo que será conveniente alargar la curva de descarga.

El motivo de necesitar entre 500-800 bits sale explicado en el artículo [1] donde justifican que, siguiendo las recomendaciones de la NIST, se realizarán 512/*e* muestras, siendo *e* la entropía por bit. Como la entropía, según las pruebas realizadas en el apartado 7 del artículo, se considera mayor o igual que 0'9, según la formula anterior se tendrían que tomar 570 bits. De todas formas, en el artículo recomiendan coger 768 bits para tener al menos 690 bits de entropía. Finalmente, estos 768 bits se comprimen en 256 bits (con SHA256, por ejemplo), siendo estos bits la cantidad necesaria para arrancar el algoritmo del PRNG.

6.1.3 MEDICIÓN DE LA CAPACIDAD PARA ALARGAR LA DESCARGA

Metodología

Con el objetivo de replicar las medidas realizadas en el artículo, según lo expuesto en los resultados del apartado anterior *6.1.2*, es imprescindible alargar el tiempo que dura la fase de descarga. Para alargar la curva se han realizado pruebas con distintas capacidades en C2, el condensador a la salida del *boost converter*. C2 es la referencia en el esquemático subido en [54] y mostrado en la Figura 11 de este documento. Los nuevos condensadores se han conectado en paralelo con el existente de 470nF, es decir, aunque se pruebe un condensador de 1,5uF la capacidad real que es de 1,97uF. La forma en la que se ha realizado dicha conexión se muestra en la Figura 4.

Las mediciones se han realizado para el circuito *m03*, el circuito en el que se identificó un tiempo de descarga menor en las medidas del apartado *6.1.1* y apartado *6.1.2*.

Resultados

Los tiempos medidos para cada capacidad añadida en C2 se muestran en la Tabla 7:

Tabla 7: Tiempos de descarga para distintas capacidades en C2

Tiempos de descarga para distintas capacidades en C2	
470 nF	1,12 ms
1,5 µF	4,08 ms
2,2 µF	5,28 ms
3,3 µF	8,08 ms
4,7 µF	9,60 ms
10 µF	32,4 ms

Se ha decidido usar el condensador de 10µF para tener tiempo suficiente de muestreo de números aleatorios válidos. Además, se ha podido comprobar que el aumento de C2 no afecta al funcionamiento del *boost converter* en la fase de carga, únicamente se alarga el tiempo de carga hasta alcanzar los 18V. Por último, hay que puntualizar que con 30ms de descarga y una frecuencia de muestreo de 128 kHz (la óptima especificada en el artículo) da tiempo a tomar 3840 muestras. De este modo, añadiendo el condensador de 10 µF se consigue un tiempo superior a los 12ms de descarga que usa en el artículo.

6.2. MEDIDAS DE LA FUENTE DE RUIDO

En esta sección se recogen las medidas que tienen el objetivo de proporcionar información sobre cómo funciona el proceso de avalancha del diodo Zener generador de ruido. El funcionamiento del diodo y su análisis teórico se desarrolla en el punto *4.2. Análisis del Generador de Ruido* de este documento. Para probar el diodo se ha usado el mismo esquema que utilizado en el punto 3.1 del artículo [1] y que se muestra en la Figura 25 de este documento.

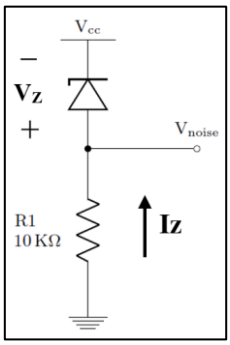


Figura 25: Esquema editado de conexión para medir el ruido del diodo

6.2.1 MEDICIÓN DEL PUNTO ÓPTIMO DE TRABAJO DE LA FUENTE DE RUIDO

Las primeras mediciones realizadas tienen el objetivo de estudiar si el punto óptimo de los diodos Zener que disponemos coincide con el expuesto en [1]. Se denomina punto óptimo a la tensión V_{HIGH} (V_{CC}) de alimentación del circuito de la Figura 25 para la cual se alcanza una tensión pico-pico máxima (ΔV_{NOISE}). Esta será la tensión para la cual el diodo generará un ruido eléctrico de mayor intensidad.

Metodología

En primer lugar, para poder estudiar el comportamiento del circuito se ha medido con el osciloscopio [51], la forma de onda de V_{NOISE} para distintos valores de V_{HIGH} fijados con la fuente de alimentación [52]. De V_{NOISE} se ha tomado su valor medio y su tensión pico-pico máxima (ΔV_{NOISE}).

También, hay que indicar que no se ha usado intervalos regulares para V_{HIGH} usando un salto en entre los valores medidos menor para las regiones más críticas:

- En el intervalo de [0 , 11] y [15'5 , 19'5] (V) se ha tomado medidas cada 1V.
- En el intervalo de (11 , 12] y (14 , 15'2] (V) se ha tomado medidas cada 0,3V.
- En el intervalo de (12 , 14] (V) se ha tomado medidas cada 0,1V.

En segundo lugar, sabemos que conociendo V_{NOISE} y V_{HIGH} se pueden calcular la Vz y Iz a partir de las siguientes ecuaciones:

(1): $V_{NOISE} = -Iz \cdot 10k$

(2): $Vz = -V_{HIGH} + V_{NOISE}$

(1)→(2): $Vz = -V_{HIGH} - Iz \cdot 10k$; $Iz = (-V_{HIGH} - Vz)/10k$

Resultados

El resultado de los valores medidos de V_{NOISE} para cada valor de entrada V_{HIGH} se han representado en la Figura 26, Figura 27 y Figura 28:

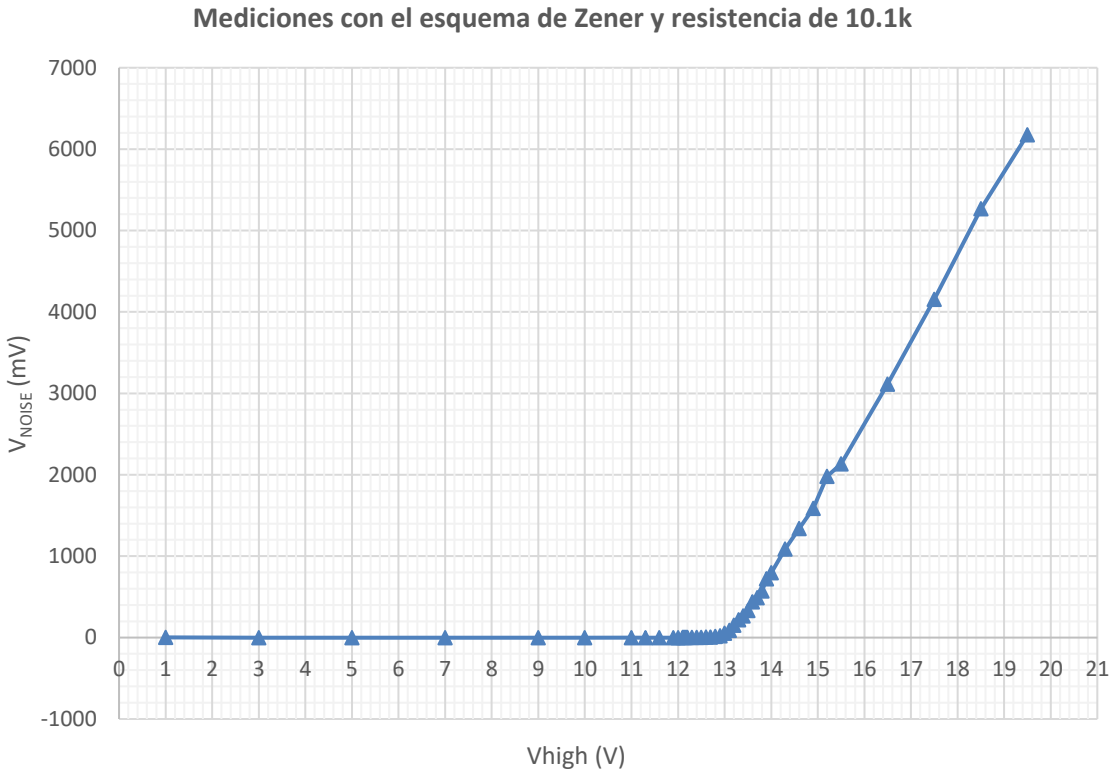


Figura 26: Gráfica de V_{NOISE} en función de V_{HIGH}

En la Figura 26 se observar que hasta que no se alcanzan casi los 13V en V_{HIGH} la tensión en V_{NOISE} es prácticamente 0V. Esto concuerda con la teoría y la datasheet porque hasta que Vz no supere la tensión Zener de *breakdown* el diodo se encontrará en estado abierto, por lo tanto, Iz es de 0mA (aprox.) y en la resistencia de 10KΩ no cae tensión.

Por otro lado, cuando V_{HIGH} es mayor de 13V el nivel medio de V_{NOISE} aumenta de forma lineal en función de $V_{HIGH,}$ ya que el diodo conduce en inversa y por lo tanto se produce una caída de tensión en la resistencia de 10kΩ.

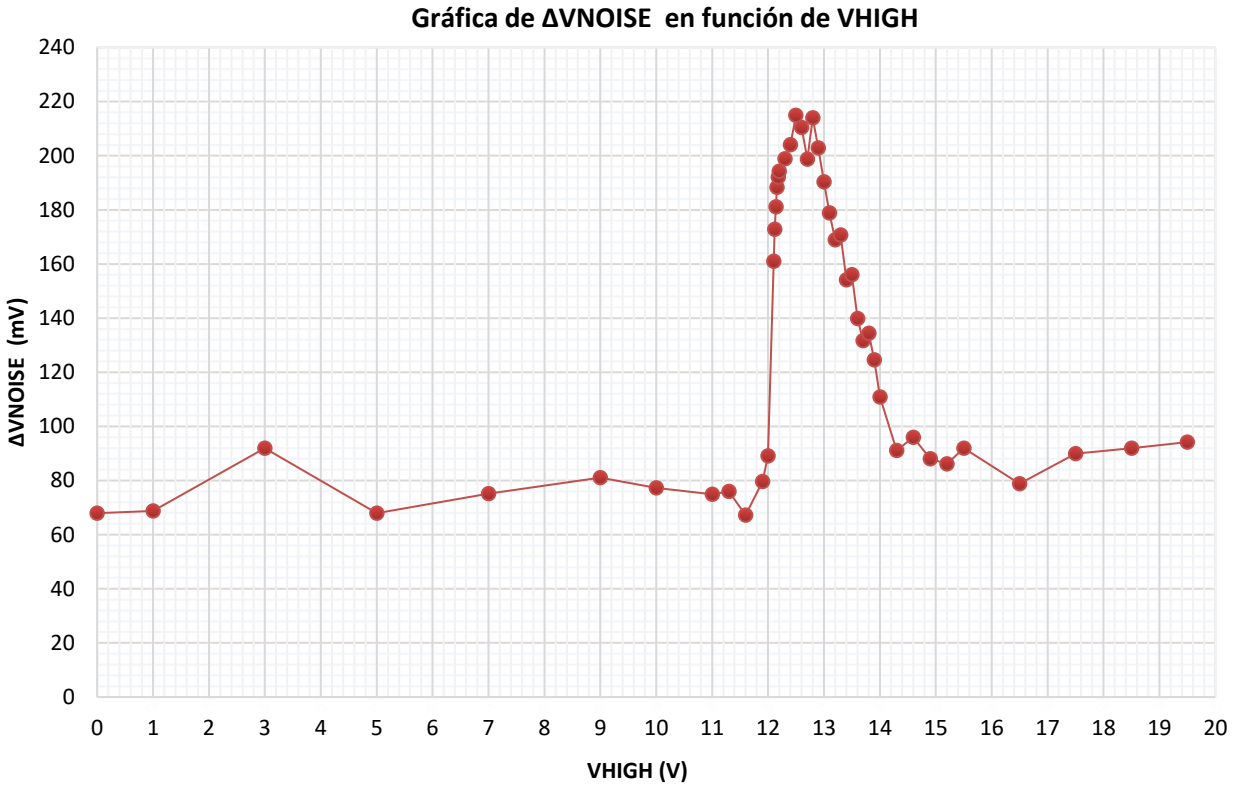


Figura 27: Gráfica de la variación de V_{NOISE} en función de V_Z

En la Figura 27, se relaciona la tensión pico-pico de V_{NOISE} (ΔV_{NOISE}) en función de V_{HIGH}. Por debajo de los 12V y por encima de los 14V, donde el diodo no se encuentra en la fase de *reverse breakdown*, ΔV_{NOISE} tiene un valor medio cercano a los 80mV (Tabla 8). Además, se ha calculado que la desviación típica[4] es de solo 6mV, por lo que se puede considerar el valor pico-pico prácticamente constante en la región por debajo de los 12V y por encima de los 14V.

Media y Deviación Típica de ΔV_{NOISE} en función de V_{HIGH}		
	ΔV_{NOISE} medio(mV)	**Desviación ΔV_{NOISE} (mV)**
V_{HIGH}<=12V	77,2	8,1
12V< V_{HIGH} <=14V	151,6	30,0
14< V_{HIGH}	89,8	5,1

Tabla 8: Media y Deviación Típica de ΔVNOISE en función de VHIGH

[4] La desviación típica es la medida de la dispersión de los valores respecto a la media (valor promedio).

Por otro lado, justo por encima de los 12V hasta los 14V observamos que ΔV_{NOISE} es de media 152mV (Tabla 8), casi el doble que cuando nos encontramos fuera de este intervalo. Pero su desviación estándar es de 30mV, cinco veces mayor. Además, si nos fijamos en la Figura 27 se observan perfectamente como $\Delta V_{NOISE\ aumenta}$ progresivamente hasta alcanzar su máximo en 214'9mV para V_{HIGH}=12'5V. Finalmente va decrementando hasta los 14V.

De estos últimos datos se puede interpretar que existe un punto óptimo en el que la intensidad del ruido es mayor, como se explica en [1]. Aunque se haya encontrado un punto óptimo este no coincide con el especificado en el artículo, de 12'16V, divergiendo en 340mV.

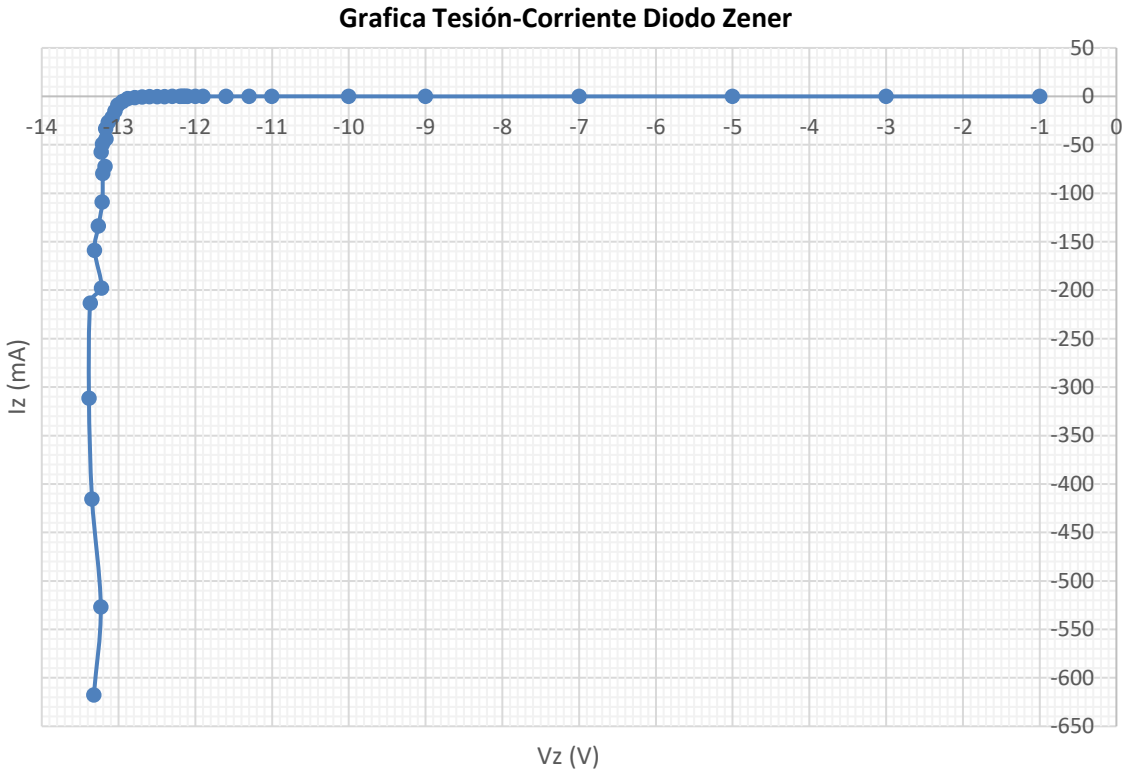


Figura 28: Gráfica Tensión-Corriente del diodo Zener

De la Figura 28: Gráfica Tensión-Corriente del diodo Zener, calculada con las ecuaciones (1) y (2), se puede identificar la curva característica de un diodo Zener lo que nos sirve como comprobación de que las medidas realizadas son coherentes. Aunque se observa como el aumento de Iz cuando el diodo se encuentra en estado de forward no es completamente lineal muestra a muestra, vemos como a medida que aumenta la tensión sigue una tendencia lineal.

En el artículo el resultado obtenido fue el de un ruido medio de 160mV con una desviación de la media de ±60mV para V_{HIGH} de 12,16V (descrito en el punto 4.2. de este documento). Mientras que, en estas medidas, para esa misma tensión, se ha obtenido un ruido medio de 0'9mV con una desviación de la media de ±94,15mV (ΔVNOISE típico/2). Estos resultados divergen de descrito en el artículo, por eso se plantea si el punto óptimo de trabajo depende del diodo escogido. Esta hipótesis se ha analizado en el punto *6.2.2 Medición de la Distribución del Ruido*.

Gracias a estas mediciones se ha podido corroborar los conocimientos teóricos que se tenían sobre los diodos Zener, además de haber podido identificar la existencia de un punto óptimo en el que el Zener genera un ruido de mayor intensidad. También, se ha observado como este punto óptimo se produce para valores de V_{HIGH} muy concretos, entre 12'5V y 12'8V. La consecuencia directa de esto es que se necesitaría una fuente de alimentación muy precisa para calibrar el punto óptimo de cada diodo. Esta problemática es la que los autores pretenden solventar con la realimentación, punto que se analiza en el apartado *6.2.3*.

6.2.2 MEDICIÓN DE LA DISTRIBUCIÓN DEL RUIDO

El objetivo de estas medidas es realizar una comparación entre la distribución del ruido documentada en el artículo [1] y representada a través de un histograma, que se muestra en la Figura 19 de este documento. La forma en la que estas medidas son adquiridas y los resultados obtenidos por sus autores están descritos en el punto *5.2 Análisis del Generador de Ruido*. Además, estas medidas se han replicado lo más fielmente la metodología descrita en [1], replicándolas en múltiples diodos distintos en busca de diferencias en la fabricación de cada uno.

Metodología

Para replicar las medidas del artículo se ha muestreado V_{NOISE} y V_{HIGH} usando el osciloscopio [51]. En este caso se ha usado el procedimiento descrito en *3.2 Metodología*, capturando las señales con *automatizacion_muestreo_diodo.m* y post procesando los gráficos con *analisis_diodo.m*. Para muestrearlas se han tomado 500.000 muestras tomadas en un intervalo de $400 \cdot 10^{-6}$ segundos; es decir, se ha usado una frecuencia de muestreo de 1'25GHz adquiriendo muestras cada 0'8ns. En el artículo toman muestras cada 1ns, pero debido a que nuestro osciloscopio solo puede muestrear a determinadas frecuencias discretas, se ha optado por la que se acerca más.

Como complemento a las medidas del artículo se ha decidido realizar las mediciones no solo de un diodo, tambien se han realizado de 10 diodos idénticos del mismo fabricante.

Resultados

Para analizar la distribución del ruido se han calculado histogramas para las medidas muestreadas de cada diodo (Figura 29) y se han recogido en la Tabla 9 la media, la desviación típica y la tensión pico-pico máxima de V_{NOISE}.

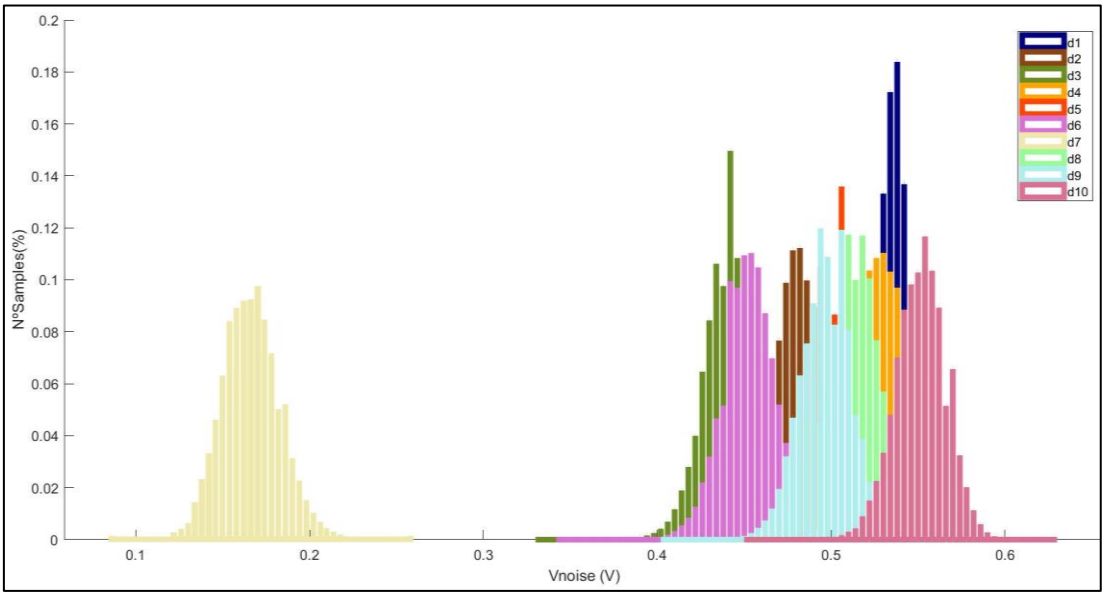


Figura 29: Histogramas del ruido generado por cada diodo

Deviación y media de V_{NOISE} para cada diodo analizado			
Código del diodo	**Media(mV)**	**Desviación típica (mV)**	**Tensión pico-pico máxima (mV)**
D01	536’6406	10’4217	152
D02	480’4672	14’8886	188
D03	439’8902	13’8374	180
D04	528’1218	14’3300	176
D05	500’8528	14’5044	164
D06	451’9434	14’8323	180
D07	166’5424	16’8165	172
D08	513’3134	14’3543	168
D09	496’5416	14’4995	168
D10	551’5818	14’7216	180

Tabla 9: Deviación y media de Vnoise para cada dido analizado

Analizando la Figura 29 podemos observar como para la mayoría de los diodos el nivel medio de V_{NOISE} es muy similar, variando entre 552mV y 440mV (según la Tabla 9). La única excepción es el ruido del diodo D07, que presenta un nivel medio bastante inferior, de 166'54mV. En cuanto a la distribución de V_{NOISE} podemos identificar la forma de una distribución normal (ver Figura 29), pero con una varianza pequeña. Si analizamos los valores de la desviación típica se encuentran todos cercanos a los 14mV, salvo D01 que es de 10mV y D07 que es de 16mV. D07 por lo tanto presenta un nivel medio menor y una variación de V_{NOISE} mayor, es decir, genera más ruido. Por otro lado, podemos identificar como la desviación típica no se encuentra directamente correlada con la tensión pico-pico máxima. Esto se ve claramente en el D07, donde la tensión pico-pico es similar a la del resto de circuitos, lo que significa que las muestras de V_{NOISE} se encuentra más repartidas que las del resto, pero alcanzan los mismos máximos absolutos.

Comparándolo con la *Figura 19: Desviación del nivel medio del ruido (Fig. 4 de)* podemos determinar que, la desviación de la media (120mV pico-pico en [1]) y la media (160mV en [1]) son algo mayores en nuestras medidas. La única excepción es D07 en la que la media es prácticamente la misma. Una explicación para estos resultados es el hecho de que no todos los diodos presenten el mismo punto óptimo de trabajo, es decir, que no todos alcancen la generación de ruido ideal para la misma tensión de alimentación V_{HIGH}. En la mayoría de los diodos, salvo D07, se identifica que hay una proporción de muestras significativamente mayor para los valores centrales de la distribución. Esto se debe evitar porque implica que la varianza del ruido no es suficiente y puede dar lugar a una correlación serie alta de los bits a la salida del circuito.

Además de analizar $V_{NOISE,}$ se ha representado la distribución de las muestras de V_{HIGH} (V_{CC}). Como se puede observar en la Figura 30, aunque la mayor parte de las muestras se encuentran en los 12'16V existe cierta varianza. Este error habrá repercutido en la generación de ruido a la vez que la propia generación de ruido habrá repercutido en que se produzca esta varianza. Esto se justifica con el propio comportamiento del diodo el cual al haberse calibrado en el punto en el que se empieza a producir el estado de *rever breakdown* se encuentra constantemente generando ruido.

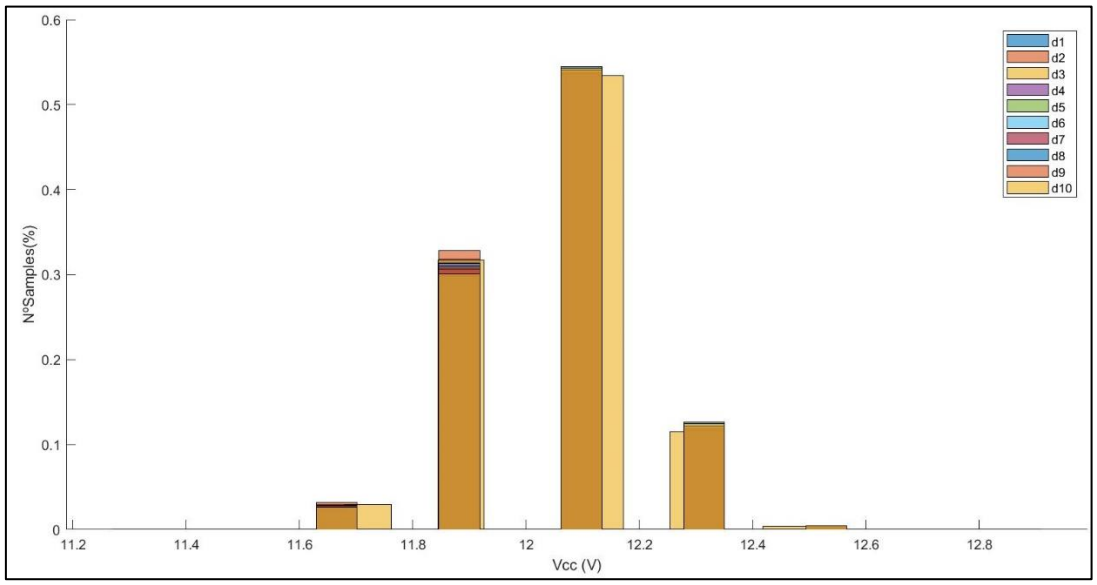


Figura 30: Histogramas de V_{HIGH} para la medición de cada diodo

Concluyendo, podemos afirmar claramente que no todos los diodos se comportan igual y que cada uno tiene un punto óptimo de trabajo. Esto sería una gran problemática si para cada circuito fabricado habría que calcular el punto óptimo de trabajo, pero como se anticipa en el punto *4.2.2* de este documento la realimentación ayuda a corregir este problema.

6.2.3 MEDICIÓN DE LAS FUENTES DEL RUIDO CON REALIMENTACIÓN

El objetivo de estas medidas es completar el análisis de la fuente de ruido realizado en [1] y en el apartado *6.2.1* y *6.2.2* de este documento analizando el comportamiento del diodo con realimentación. Para ello se ha medido V_{NOISE}, justo a la entrada de la realimentación, en los propios circuitos fabricados.

Metodología

Se han muestreado la salida de cada fuente de ruido (*NOISE1* y *NOISE2*), junto con la salida final aleatoria del circuito (*OUT*). Además de las señales anteriores, se ha muestreado la señal que en [1] llaman V_{REF}. Se trata de la tensión que fija el diodo Schottky en la entrada positiva de los dos operacionales que forman parte de las fuentes de ruido. Todas las medidas se han realizado sobre un circuito de cada fabricante (*e05, m02, s02* y *w01*).

El *enable* se ha realizado con una señal cuadrada de 3V en *high* y 0V en *low*. La señal tiene un periodo de 40ms y el estado de *high* dura 8ms, tiempo suficiente para que se cargue al máximo el condensador. Es importante aclara que para estas medidas se ha incrementado al condensador C2 en 10µF, justificado en el punto *6.1. Medidas de la Fase de Descarga*. Finalmente, el circuito se ha alimentado con 3'3V±0'1V.

La forma en la que se han realizado las conexiones entre el circuito y el osciloscopio se muestran en la Figura 31. Las sondas se han enganchado al ánodo de cada diodo generador de ruido, es decir, a la salida de cada fuente de ruido. La sonda del canal 3 del osciloscopio se ha usado para *NOISE2* y la del canal 4 para *NOISE1*. Para la conexión con V_{REF} se ha necesita soldar un tramo de hilo de *wrapping*.

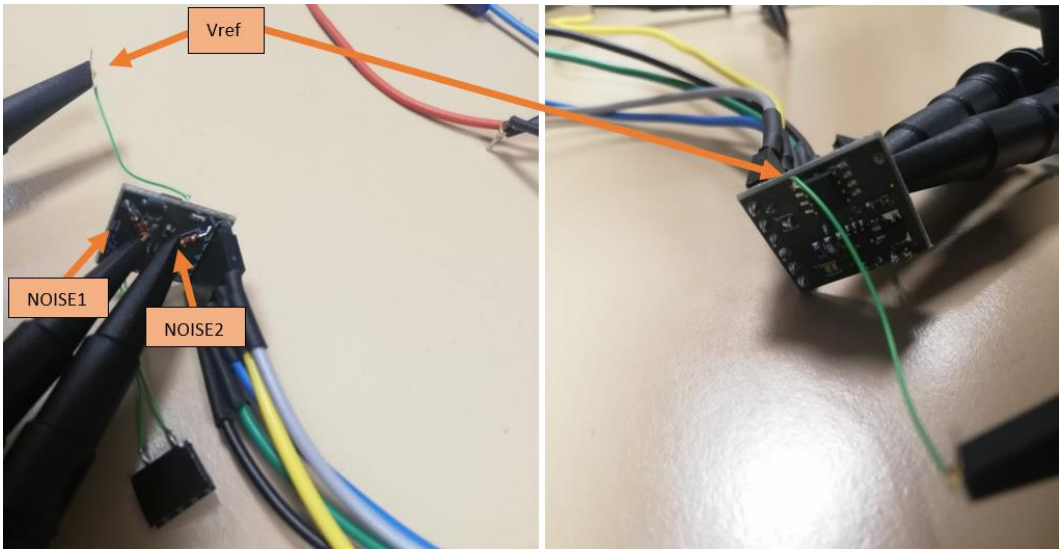


Figura 31: Conexiones de la para medir NOISE2, NOISE1 y V_{REF}

Las señales se han muestreado y postprocesado con un el script de MATLAB *procesarSenalesAleatorias.m*. Se han usado las siguientes variables para almacenar las señales muestreadas: la sonda de la izquierda (*NOISE2*) y la de la derecha (*NOISE1)* en *aleatorySignalIZQ* y *aleatorySignalDER* respectivamente, y en *vRefSignal* la tensión V_{REF}. El muestreo se ha realizado a 12'5MHz y la franja de adquisición de muestras ha sido entre el flanco de bajada de la señal de *enable* y los siguientes 28ms. Ha sido necesario dejar un margen de 4ms (el periodo de *enable* es de 40ms y se encuentra activado durante 8ms) con el *enable* desactivado, porque la entropía de la salida aleatoria decrecía.

Resultados

En la Figura 32 se muestran los valores del nivel medio de cada señal muestreada además de la diferencia del nivel medio de las dos fuentes de ruido.

Nivel medio para cada señal aleatoria (V) (con enable)

Fabricante	OUT	NOISE1	NOISE2	NOISE1-NOISE2	VRef
European Circuits	1.584	0.267	0.2445	0.02258	0.1943
Micron20	1.299	0.2367	0.2111	0.02557	0.1519
Shenzhen	1.44	0.273	0.2463	0.02668	0.1928
Wurth	1.57	0.2727	0.2519	0.02075	0.1957
MEDIA	1.473	0.2623	0.2385	0.02389	0.1837

Figura 32: Nivel medio para cada Fuente de Ruido

Podemos ver cómo, para todos los circuitos medidos, el nivel medio de *NOISE1* es mayor que el de *NOISE2*. En cuanto a la diferencia entre ambas señales (*NOISE1-NOISE2*), se encuentra en el rango de los 20 – 27mV. No podemos anticipar si esta diferencia puede afectar significativamente a la salida aleatoria del circuito, pero hay que destacar que la diferencia es siempre positiva (NOISE1 es siempre mayor que NOISE2). Es importante puntualizar que esta diferencia no está provocada por factores externos al circuito como pueden ser las sondas usadas para el osciloscopio, ya que se han realizado pruebas con diversas sondas y en distintos canales del osciloscopio y el resultado ha sido el mismo.

En cuanto a V_{REF} vemos como es de media 78,6mV menor que *NOISE1* y 54.8mV que *NOISE2*. Esta diferencia, según se expone en el artículo (explicado en el punto *4.2.2* de este documento), tendría que ser de 0mV aproximadamente, ya que la realimentación negativa tiende a alcanzar la tensión de referencia de entrada (V_{REF}) en la salida.

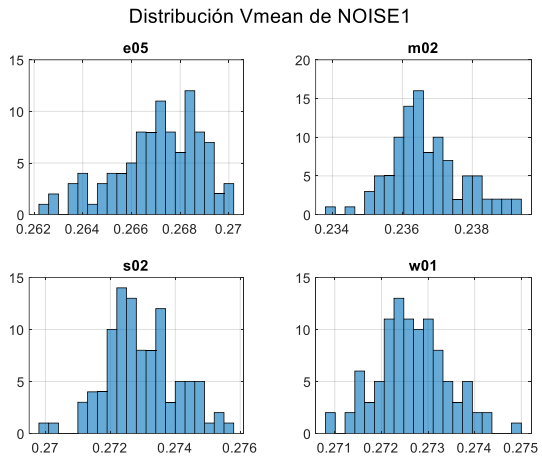


Figura 33: Histograma del nivel medio de NOISE1

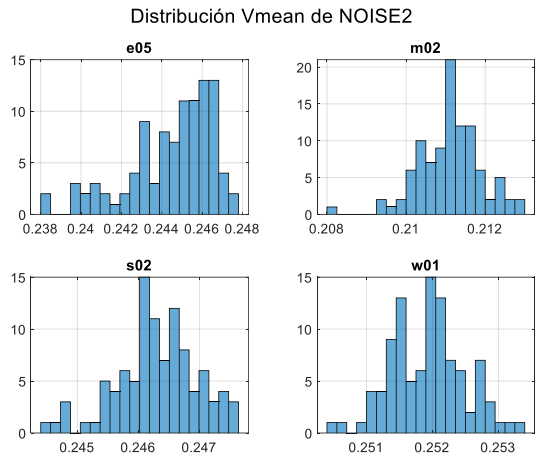


Figura 34: Histograma del nivel medio de NOISE2

Al comparar la desviación del nivel medio para cada circuito (Figuras Figura 33 y Figura 34, donde el eje *y* muestra el número de ciclos y el eje *x* la tensión en V_{NOISE}), vemos como es aproximadamente la misma para todos los circuitos (de 10mV).

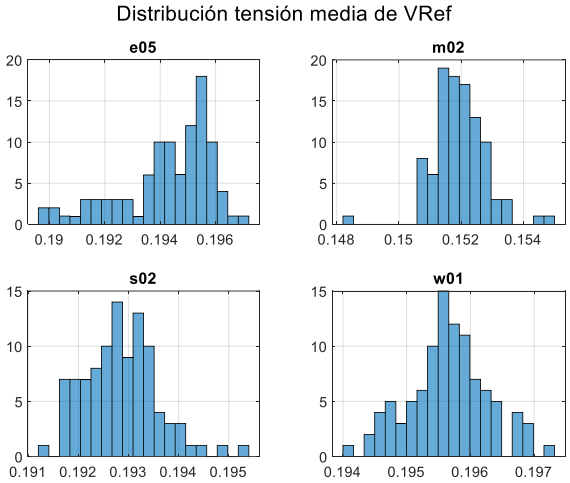


Figura 35: Histograma del nivel medio de Vref

Para el caso de V_{REF} , hay una desviación típica de V_{REF} de 5mV. Esta desviación, aunque es menor que la de *NOISE1* y *NOISE2* debería ser de 0mV, ya que la tensión de referencia no debería cambiar. En este caso se plantea que dicha variación puede ser debida a que se esté propagando el ruido generado por los diodos no solo por la señal *NOISE1* y *NOISE2*, sino que también, por el resto de las pistas del circuito.

Después de realizar el análisis podemos afirmar que:

- Los niveles medios son similares para los distintos circuitos de cada fabricante.
- Las diferencias entre los niveles medios de las dos fuentes de ruido son aproximadamente constantes.
- La tensión media de V_{REF} es menor que la de *NOISE1* y *NOISE2* en todas las mediciones.
- La variación entre los niveles medios de una misma fuente de ruido es pequeña y constante para los distintos circuitos medidos.
- La variación de V_{REF} es de 5mV, a pesar de que esta debería ser prácticamente de 0mV.

Como conclusión podemos afirmar, en primer lugar, que el bucle de realimentación está funcionando en el sentido de que se están alcanzando niveles medios similares para circuitos de distintos fabricantes. Por lo tanto, se están corrigiendo con la realimentación los posibles sesgos introducidos por cada diodo, que se han identificado en el punto *6.2.2 Medición de la Distribución del Ruido*.

En segundo lugar, afirmamos que no se está cumpliendo el principio descrito en el artículo por el cual el nivel medio de las fuentes de ruido debe ser la tensión de referencia V_{REF}. Además, identificamos que los niveles medios de las dos fuentes de ruido son distintos entre sí, lo que también rompe el principio descrito en él punto *4.3. Análisis del Comparador Final*. En este apartado se explica que es imprescindible que el nivel medio de las dos fuentes de ruido sea el mismo, para que al restarlos en el comparador, se anulen en la salida y no se vea afectada la entropía de la salida.

El hecho de que estas discrepancias con respecto a lo descrito en el artículo [1] se hayan observado para circuitos de distintos fabricantes, en medidas tomadas en distintos días y con distintas configuraciones, nos permite concluir que se trata de un sesgo producido por la forma en la que está concebido el circuito y no por un problema en la fabricación o en las tolerancias de los componentes.

6.3. MEDIDAS DE LA SALIDA PARA DISTINTAS FRECUENCIAS

En esta sección se analizan las medidas realizadas con el objetivo de estudiar cómo afecta la frecuencia de muestreo a la salida aleatoria del circuito. Dicho análisis se hace en base a lo descrito en el punto *7.1 Establishing sample rate* de [1]. Por ello se replicarán las medidas realizadas en artículo completándolas mediante diversas representaciones

En el artículo se basaron en la entropía y la correlación serie por bit para calcular la frecuencia óptima de muestreo con la que conseguir una secuencia de bits lo más aleatoria posible. El cálculo de estos dos parámetros se realizó con el software estadístico *ENT Test Suite* [59]. En cuanto al muestreo se tomaron 500.000 muestras para tres frecuencias distintas: 100kHz, 10MHz y 500MHz. El cálculo de las señales intermedias se realizó en el postprocesado diezmando las señales originales. Los resultados se muestran en las Figura 36 y Figura 37:

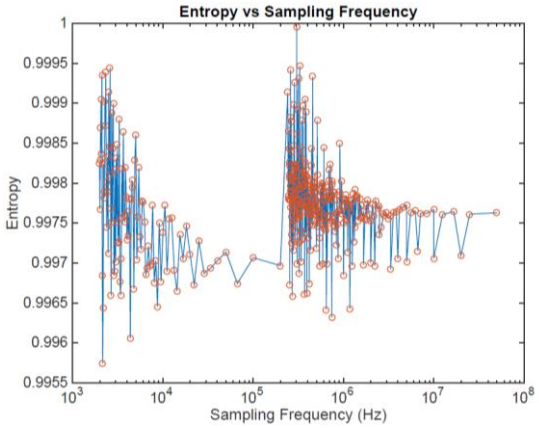


Figura 36: Entropía en función de la Frecuencia (Fig. 12 de [1])

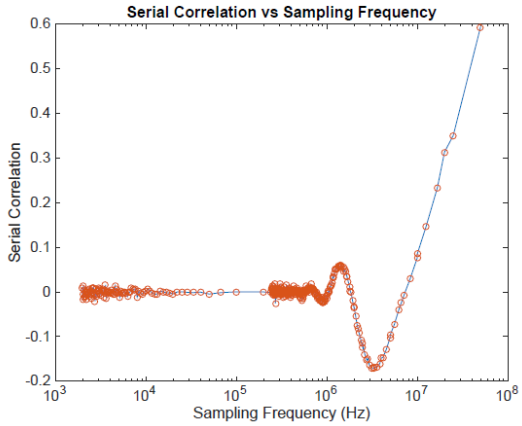


Figura 37: Correlación Serie por bit en función de la Frecuencia (Fig. 13 de [1])

Las conclusiones a las que llegan en el artículo es que la frecuencia máxima de muestreo recomendada es de 6MHz donde la correlación serie por bit sobrepasa los 0'5. Además, identifican que la frecuencia óptima de muestreo es 128kHz, donde argumentan que se encuentra el equilibrio entre una entropía elevada y una correlación serie mínima.

Tras realizar nuestro propio análisis de sus resultados, nos llama la atención el hecho de que la desviación típica de la entropía y la correlación serie aumente a raíz que aumenta el factor de diezmado. Además, el incremento de la desviación (más notorio en la gráfica de la entropía) se corrige cuando se pasa a diezmar desde una señal muestreada a otra frecuencia. Por ejemplo, en la Figura 36 la máxima desviación típica sucede justo para las frecuencias mayores que 100kHz, pero una vez se pasa al rango de las frecuencias diezmadas desde 100kHZ (frecuencias menores que 100kHz) la desviación típica es prácticamente nula. A raíz de estas observaciones se plantea si el diezmado digital puede estar afectando significativamente a la aleatoriedad.

6.3.1 ANÁLISIS DIEZMANDO DESDE 12.5MHZ

En estas mediciones se realiza una primera aproximación para contrastar los resultados experimentales con en el punto 7.1 de [1]. Las medidas se han realizado para el circuito *w04*, previamente preseleccionado por presentar una entropía y correlación serie elevada.

Metodología

Para estas mediciones se ha usado una única frecuencia de muestreo de 12'5MHz que posteriormente se ha diezmado para abarcar todo el rango de medidas de análisis, de 12'5MHz hasta 1kHz. El osciloscopio ha capturado las señales en modo *AC*, es decir, ha aplicado un filtro paso alto eliminando el nivel medio. Se han muestreado 500 ciclos de *enable on/enable off* (ciclos de 40ms), de los cuales se han tomado 28ms de la salida aleatoria para el post procesado. Al a ver muestreado a 12'5MHz de cada ciclo se han podido extraer 350.000 muestras[5], que suman un total de 175M de muestras. Aunque parezca una cifra exagerada de muestras (comparándolas con las 500.000 usadas en [1]), al diezmar hasta 1kHz ese número se reduce a 14.000 muestras. Para el postprocesado se han concatenado todos los bits escogidos de cada ciclo en un único vector.

El proceso de muestreo se ha realizado con el script *automatizacion_muestreo_estandar.m*, donde se han capturado los 500 ciclos esperando 1s para muestrear el siguiente ciclo de muestreo. De esta forma nos aseguramos de que no exista correlación entre los capturado durante un ciclo y su ciclo anterior. Para el postprocesado se ha usado el script *analisis_frecuencia.m*, para realizar el cálculo de la entropía y la correlación serie, y *analisis_diezmado.m*, para la representación del resto de gráficas realizadas después del diezmado, pero antes de la conversión a bits.

Por último, hay que indicar que en el caso de la entropía y la correlación serie se han probado dos métodos distintos para convertir la señal muestreada (discretizada en el muestreo pero con valores decimales), en valores binarios. Para realizar el proceso es necesario establecer un criterio para distinguir entre un 1 o un 0, en este caso al haber capturado las señales en *AC*, el nivel medio debería ser de 0V siendo este uno de los criterios. El otro criterio es fijar un nivel igual a la media de la señal una vez diezmada.

[5] Se ha calculado multiplicando la frecuencia de muestreo de 12'5MHz por el tiempo configurado para capturar bits, en este caso de 28ms. Se toman 28ms, porque el periodo del *enable* es de 40ms, el tiempo de carga es de 8ms y los 4ms restantes es el margen dejado en el que la aleatoriedad de la salida decrementa.

Análisis Entropía

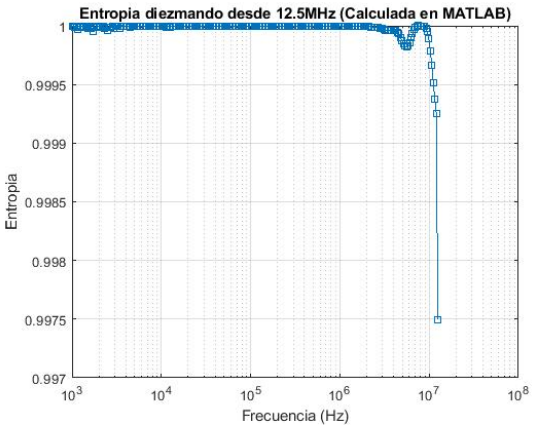


Figura 38: Entropía ajustando el nivel medio desde 12.5MHz

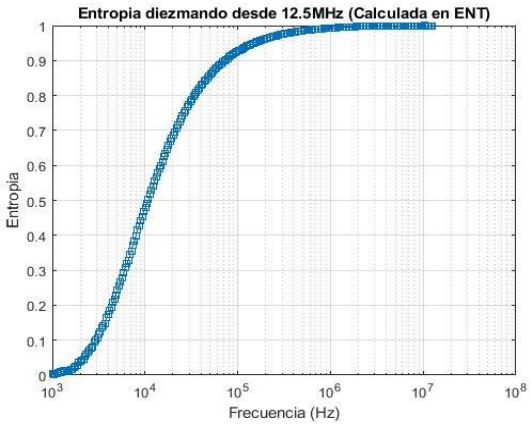


Figura 39: Entropía con nivel medio fijo a 0V desde 12.5MHz

En la Figura 38 se puede observar cómo ajustando el nivel medio después del diezmado se consiguen entropías prácticamente ideales, iguales a 1 o muy cercanas a 1. Lo que significa que existe una proporción ideal de 0’5 de unos y ceros. Por otro lado, esto nos sucede para las frecuencias en las que existe un factor de diezmado menor (las mayores), lo que nos lleva a pensar que, aunque se ajuste la media, existen valores a típicos que tras diezmar desaparecen. A pesar de esto, una entropía de 0’9975 sigue siendo una entropía muy elevada.

En el caso de la Figura 39, vemos como si usamos como nivel 0V la entropía cae drásticamente hasta casi alcanzar un valor de 0, lo que significa que toda la secuencia son unos o ceros. Por qué se produce se ha analizado en los siguientes subapartados de estas medidas (*Análisis FFT* y *Análisis en el Dominio del Tiempo*).

Se podría argumentar que el decremento de la entropía se debe al error cometido por estar usando cantidades distintas de muestras para calcular la entropía en cada frecuencia, ya que a medida que se diezma el número de muestras se reduce. Para descartar esta hipótesis se han realzado las mismas gráficas, pero para el mismo número de muestras independientemente de la frecuencia de diezmado. Se han cogido para todas las frecuencias las 14.000 primeras muestras, las resultantes cuando se aplica el máximo factor de diezmado.

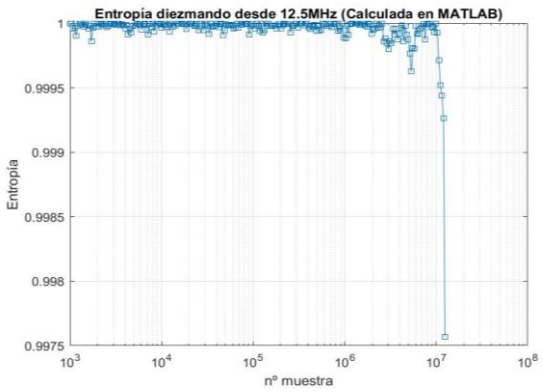


Figura 40: Entropía ajustando el nivel medio desde 12.5MHz para 14.000 muestras

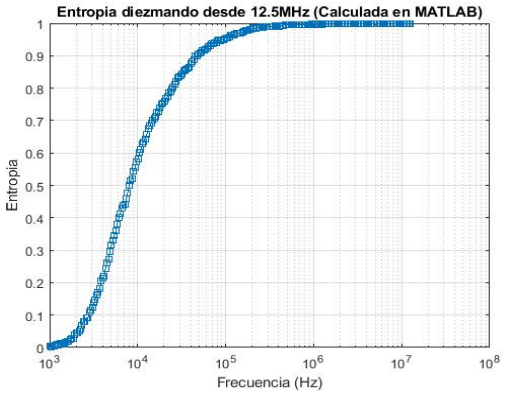


Figura 41: Entropía con nivel medio fijo a 0V desde 12.5MHz para 14.000 muestras

Se puede observar como las Figura 40 y Figura 41 son prácticamente idénticas a Figura 38 y Figura 39. La única diferencia apreciable es que para este caso existe una desviación mayor. Debido a esto se descarta completamente la hipótesis de que sea un error por usar distinto número de muestras.

Análisis Correlación Serie

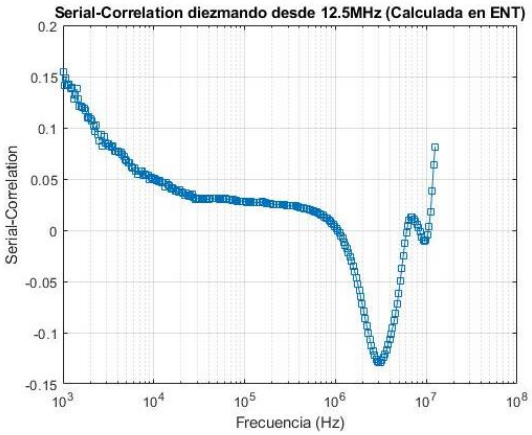


Figura 42: Correlación Serie ajustando el nivel medio desde 12.5MHz

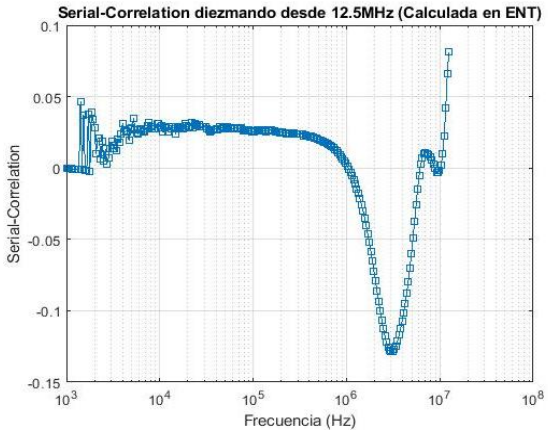


Figura 43: Correlación Serie con nivel medio fijo a 0V desde 12.5MHz

En la Figura 42 se identifica una forma similar a los resultados obtenidos en [1] mostrados en la Figura 37. La principal diferencia es que para las frecuencias más bajas la correlación serie decrementa alcanzando 0'15. En cuanto a la Figura 43 no se produce el incremento de la correlación para las frecuencias menores, alcanzando un valor entrono al 0'5, muy similar a los de la Figura 37.

Con el objetivo de arrojar luz sobre el decremento de la entropía y el aumento de la correlación serie al diezma se ha realizado una serie de representaciones adicionales.

Análisis FFT

En este apartado se ha representado la Transformada Discreta de Fourier (FFT) para distintas frecuencias:

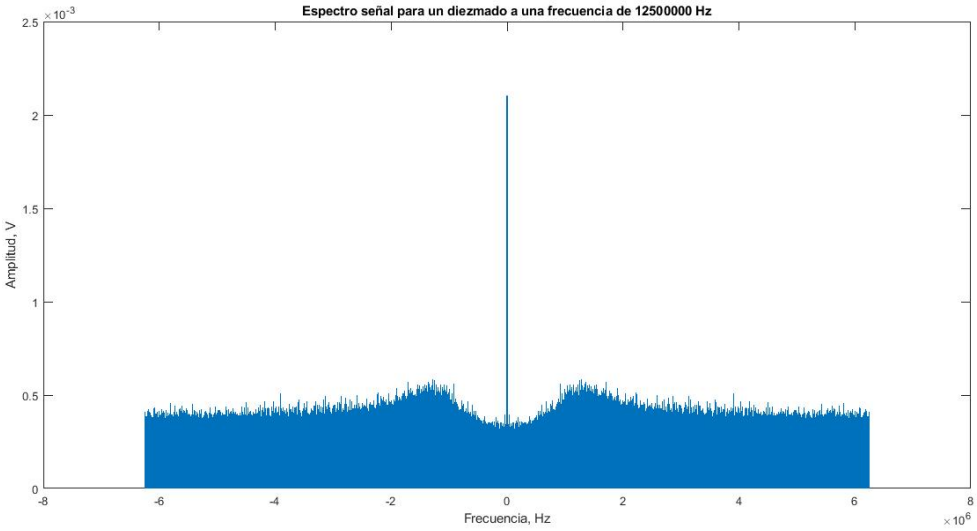


Figura 44: FFT de la señal muestreada a 12'5MHz

En la Figura 44 se representa la FFT de la señal sin diezmar, se puede observar como el espectro de la señal es bastante uniforme, exceptuando que para 1'5MHz presenta un máximo de 0'5mV y para las frecuencias próximas al 0 un mínimo. Para las frecuencias mayores de 1'5MHz la amplitud es de 0'5-0'4mV, mientras que para las menores decrece hasta 0'3mV.

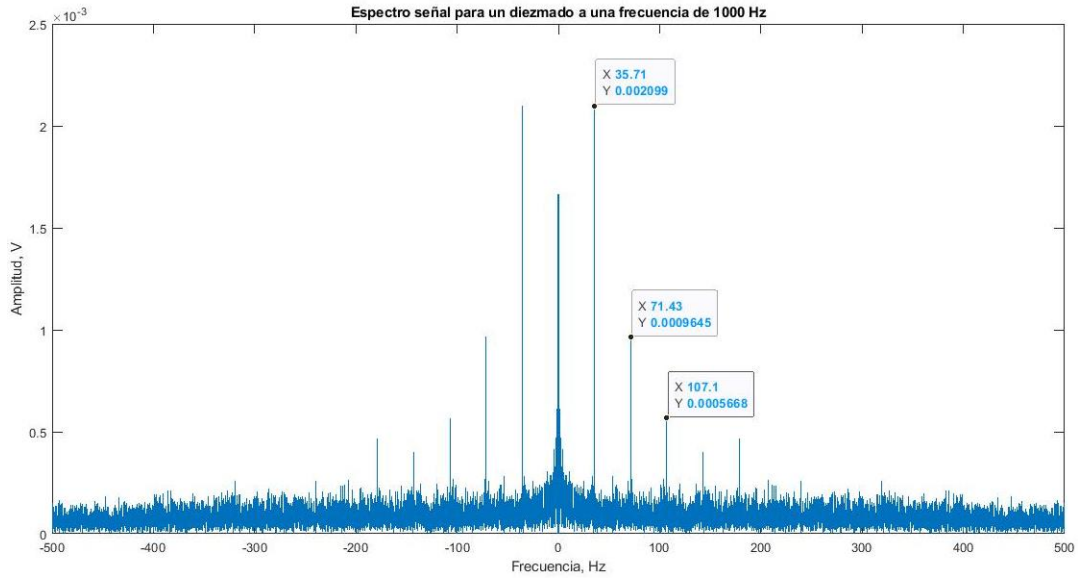


Figura 45: FFT de la señal diezmada hasta 1kHz

Al diezmar hasta 1kHz la densidad y la amplitud de la señal se reduce significativamente pasando a ser de media 0'1-0'2mV (Figura 45). Esta amplitud es menor que la observada en la Figura 44, lo que lleva a pensar que al muestrear a altas frecuencias y posteriormente diezmar se está perdiendo gran parte de la densidad de la señal aleatorio. Otra posible razón podría ser que el circuito a bajas frecuencias genere una señal aleatoria de menor densidad, esto último se estudia en el punto *6.3.2.*

Por otro lado, Figura 45 se han identificado deltas de mayor intensidad que el ruido uniforme a 35'7Hz y sus correspondientes armónicos a 71'4Hz, 107'1Hz, etc. Estos armónicos podrían estar generados por el propio circuito, pero al desacoplar el GND del osciloscopio, del generador de señales y de la fuente de alimentación se atenuaron en gran medida. Finalmente, se identificó que se trataba de la señal de un PLC del laboratorio que transmite información a través de la red eléctrica, al desconectar estos dispositivos los armónicos desaparecieron. Es importante destacar que este rudo adicional se ha filtrado a través de la alimentación del circuito y dado que el circuito no presenta ningún mecanismo elaborado para eliminarlo se propago hasta la salida aleatoria. Si no se corrige podría dar lugar a futuros ataques con el objetivo de reducir la aleatoriedad.

Análisis PDS

Analizando la *Power Spectral Density* se ha corroborado el decremento de la densidad de la señal, así como, la identificación del ruido introducido por el PLC:

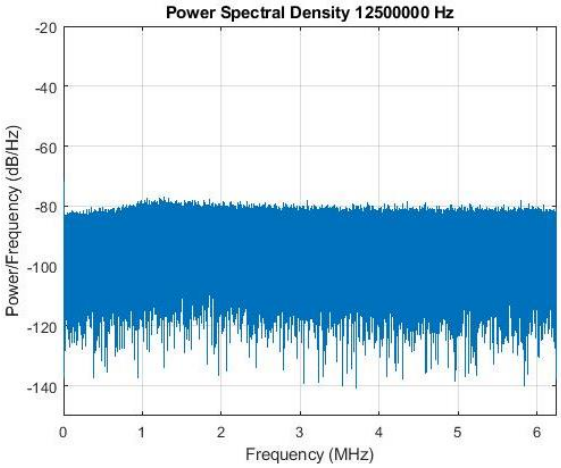


Figura 46: PDS de la señal muestreada a 12'5MHz

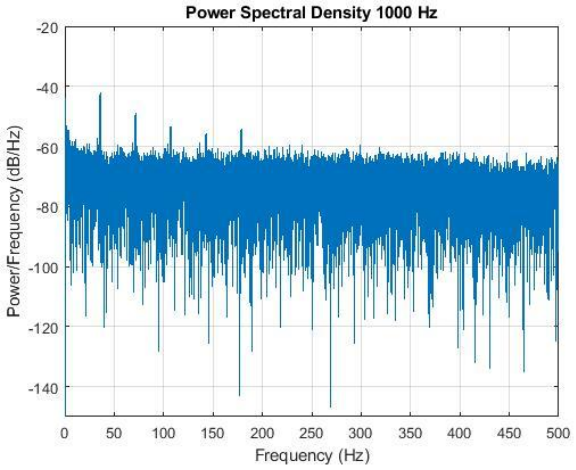


Figura 47: PDS de la señal diezmada hasta 1kHz

Análisis en el Dominio del Tiempo

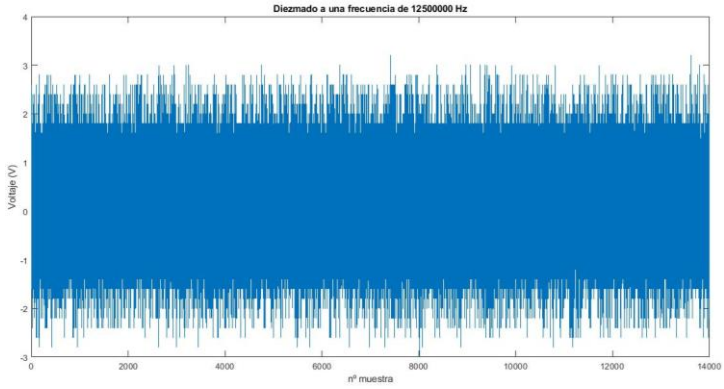


Figura 48: Dominio del Tiempo de la señal muestreada a 12'5MHz

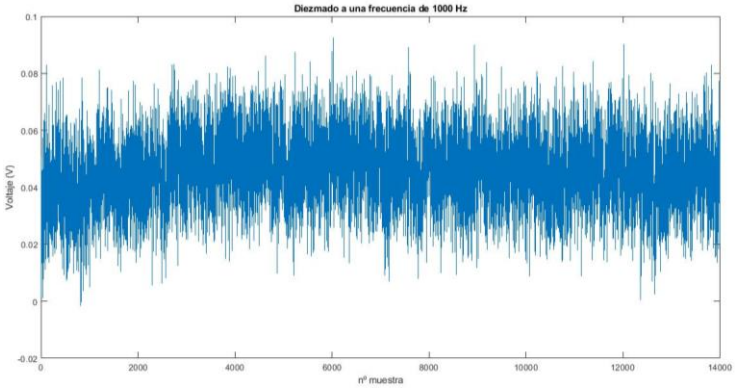


Figura 49: Dominio del Tiempo de la señal diezmada hasta 1kHz

Al compara la señal sin diezmar (Figura 48) con la diezmada hasta 1kHz (Figura 49), se ve claramente como la amplitud disminuye drásticamente, pasando de abarcar el rango de 3V hasta -3V a simplemente de 0,08V hasta 0,02V. No solo se está atenuando si o que también su nivel medio aumenta quedando por encima de 0V prácticamente todas las muestras. Esto explica que la entropía decrezca hasta 0 según aumenta el factor de diezmado (Figura 39).

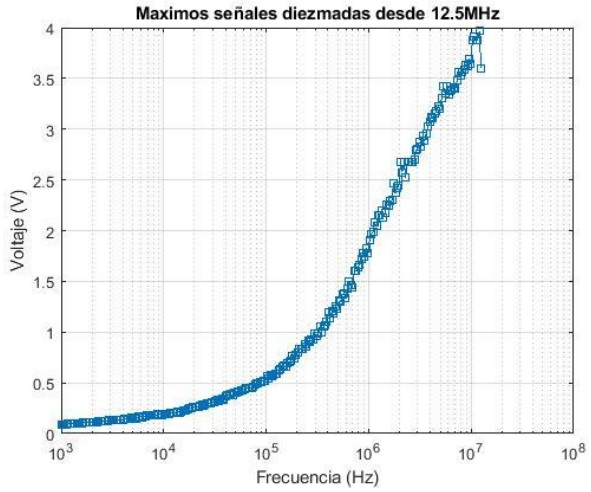


Figura 50: Atenuación en función de la Frecuencia

Por último, se ha representado los máximos para cada frecuencia de diezmado (Figura 50). Como se puede observar a medida que aumenta el diezmado el nivel medio de la señal aleatoria aumenta.

6.3.2 ANÁLISIS DIEZMANDO DESDE MÚLTIPLES FRECUENCIAS

A continuación de describen las mediciones planteadas para analizar la problemática del incremento del nivel medio al diezmar identificados en el punto *6.3.1*. Además, se estudia si eliminando la influencia del diezmado se obtiene una salida de alta entropías y con bits poco correlados. Las medidas se han realizado para el circuito *w04*, previamente preseleccionado por presentar una entropía y correlación serie elevada.

Para estas medidas se ha buscado evitar cualquier ruido externo al circuito que se pueda llegar a acoplar al propio generado por el circuito, como se identificó en el punto *6.3.1* en la Figura 45. En primer lugar, se han desconectado de la red los dispositivos PLC del laboratorio. En segundo lugar, se ha desacoplado el GND del osciloscopio, del generador de señales y de la fuente de alimentación de la red, para evitar cualquier introducción de ruido externo en el circuito.

Metodología

Para estas mediciones se ha realizado un muestreo del circuito para cada una de estas frecuencias: 12.5k, 50k, 125k, 250k, 500k, 1.25M, 2.5M, 6.25M, 12.5M, 25M y 50M. Para analizar las frecuencias intermedias, al igual que en el punto *6.3.1.*, se ha diezmado en el postprocesado hasta 1kHz. En este caso se ha configurado el osciloscopio para que capture las señales en modo *DC*, para de este modo hacer un análisis más detallado de los niveles medios.

En este caso se ha automatizado en *automatizacion_muestreo_multiples_frec.m* la captura del número de ciclos, de tal forma que para cada frecuencia de muestreo se han realizado los ciclos necesarios para superar 10M de muestras. Después en el postprocesado, el número de muestras se reduce una vez escogidas las muestras útiles dentro de cada ciclo y realizado el diezmado. Para todas las frecuencias se ha calculado la entropía y la correlación serie para más 3.5M de muestras.

Para el postprocesado se ha usado el script *analisis_frecuencia_Fs_multiple.m*, para realizar el cálculo de la entropía y la correlación serie, y *analisis_diezmado_Fs_multiple.m*, para la representación del resto de gráficas realizadas después del diezmado, pero antes de la conversión a bits. En este caso, como en el punto *6.3.1.*, se han probado dos métodos distintos para convertir la señal muestreada (discreta pero con valores decimales), en valores binarios. La única diferencia es que, al haber capturado las señales en *DC* el nivel medio fijo será de 1’65V y no de 0V.

Análisis Entropía

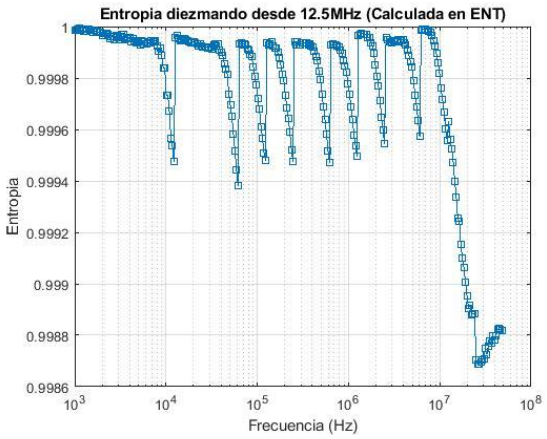


Figura 51: Entropía ajustando el nivel medio desde múltiples frecuencias

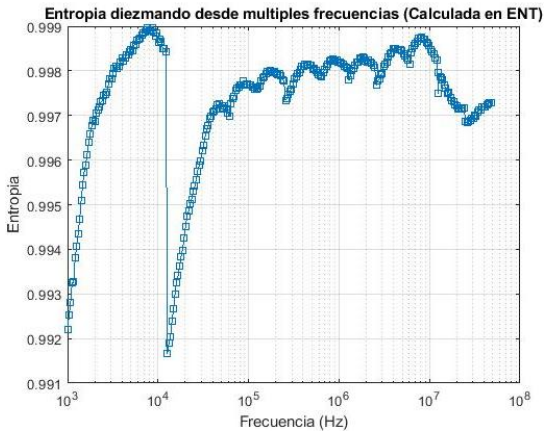


Figura 52: Entropía con nivel medio fijo a 1’65V desde múltiples frecuencias

En la Figura 51 se puede observar cómo, al igual que en el punto *6.3.1*, ajustando el nivel medio después del diezmado la entropía aumenta a medida que aumenta el factor de diezmado. Por otro lado, para el caso de la Figura 52 sucede lo opuesto, la entropía se reduce al incrementar el nivel medio al diezmar. Si nos fijamos únicamente en los Figura 52 en las entropías correspondientes a las señales sin diezmar vemos como se encuentran todas por encima 0'997, siendo las más baja para 50kHz y 25MHz. Por lo tanto, podemos afirmar que la entropía no se está viendo afectada prácticamente muestreando para un rango que llega hasta los 50MHz.

También se puede concluir que el decremento de la entropía observado en el punto *6.3.1*, ha sido claramente por el proceso de diezmado y no debido a que el circuito produzca entropías menores a bajas frecuencias.

Análisis Correlación Serie

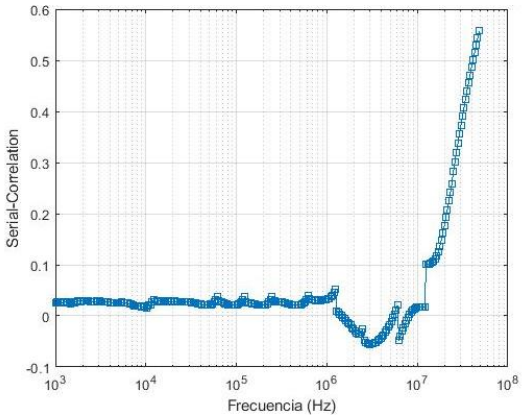


Figura 53: Correlación Serie ajustando el nivel medio desde múltiples frecuencias

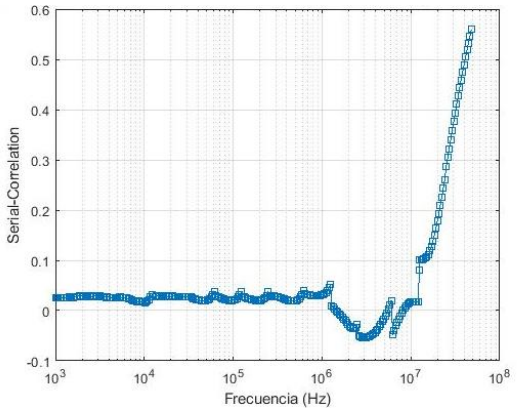


Figura 54: Correlación Serie con nivel medio fijo a 1'65V desde múltiples frecuencias

En la Figura 53 y Figura 54 se identifica una forma similar a los resultados obtenidos en [1] mostrados en la Figura 37 y en las mediciones anteriores (Figura 42 y Figura 43). Hay que destacar las discontinuidades que se producen entre cada rango de diezmado, debido al mismo motivo expuesto con anterioridad del incremento de nivel medio al diezmar. Comparándolo con la Figura 37 una diferencia es que mientras la correlación serie calculada en el artículo para las frecuencias menores se encuentra centrada en el 0, en nuestros resultados es algo mayor al estar centrada en el 0'03.

Análisis FFT

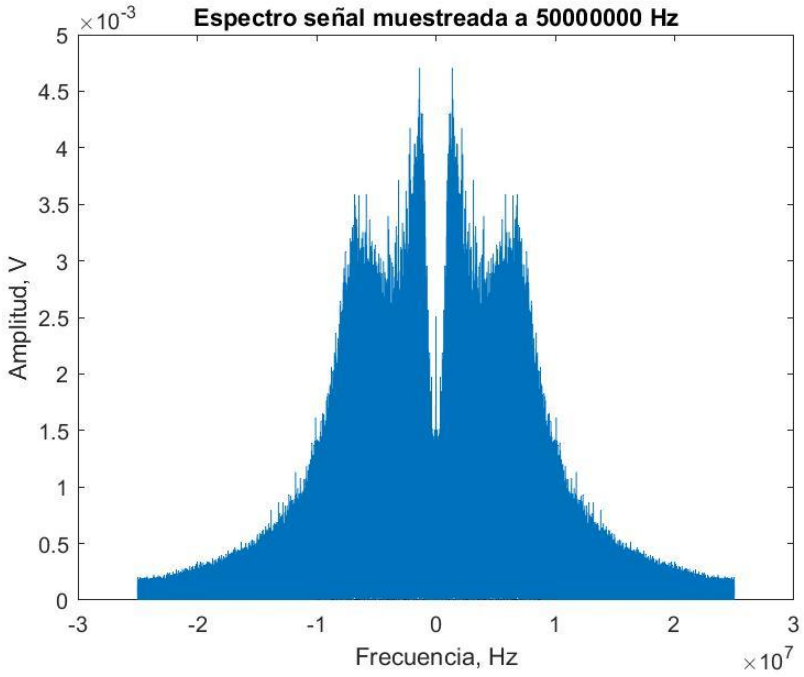


Figura 55: FFT de la señal muestreada a 50MHz

Analizando la Figura 55 se ve como a partir de los 7MHz la amplitud del ruido disminuye drásticamente (en el artículo justifican que la frecuencia máxima es de 6MHz basándose en la Figura 37). Aunque podríamos considerar esta frecuencia como la máxima a la que se debería muestrear el circuito, el espectro no llega a ser plano condición necesaria para conseguir un ruido blanco. Esto además es coherente con la Figura 54 de Correlación Serie en la que se muestra como para 7MHz la correlación sigue siendo elevada.

Debido a esto se recomienda no muestrear a más de 1.25MHz, punto en la que el espectro de la señal es completamente plano como se muestra en la Figura 56. Además, es en esta frecuencia en la que la correlación es prácticamente nula como se muestra en la Figura 54.

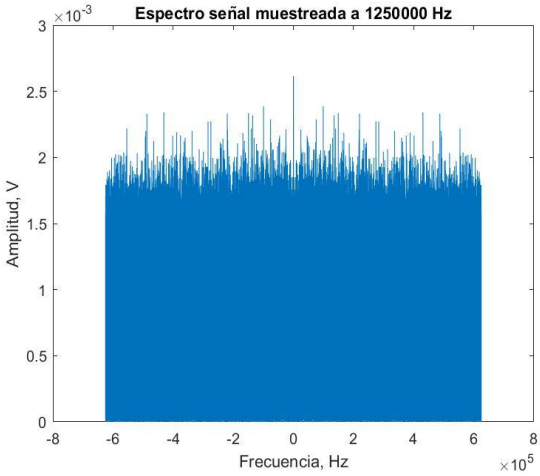


Figura 56: FFT de la señal muestreada a 1'25MHz

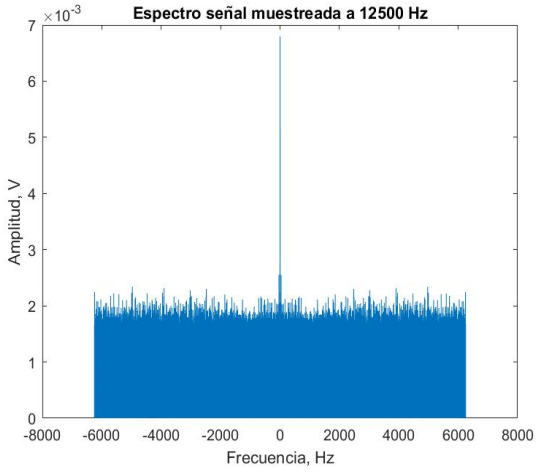


Figura 57: FFT de la señal muestreada a 1'25kHz

Finalmente, contrastando la Figura 57 con la Figura 56 se ve como la amplitud del ruido es la misma, de 2mV. Con esto se puede concluir que la atenuación de la amplitud de la señal a medida que se reducía la frecuencia de analisis, identificado en *6.3.1 Análisis Diezmando desde 12.5MHz,* se produce debido al diezmado digital de la señal. No se produce porque el circuito este generando una salida aleatoria de menor intensidad para frecuencias bajas.

Análisis PDS

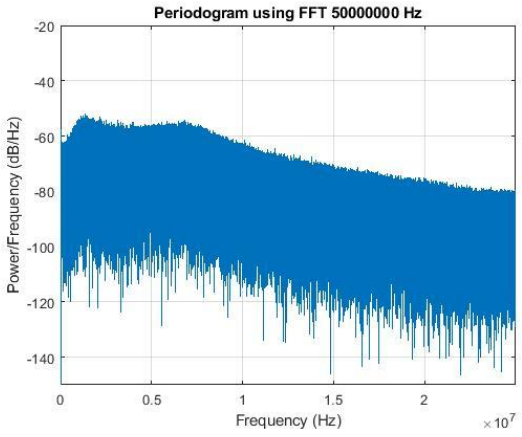


Figura 58: PDS de la señal muestreada a 50MHz

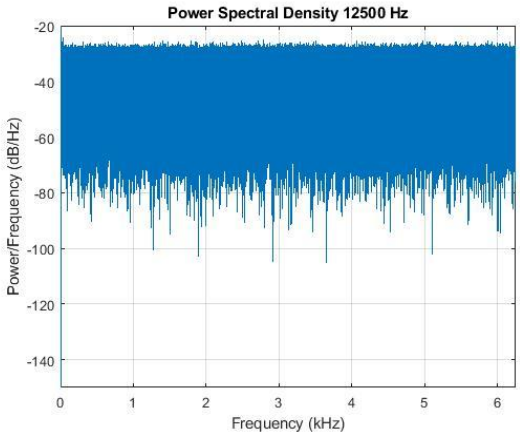


Figura 59: PDS de la señal muestreada a 12'5kHz

En este caso, a diferencia de lo identificado en *6.3.1 Análisis Diezmando desde 12.5MHz,* se observa como la densidad espectral de potencia para 12'5kHz es similar a la de 50MHz, aunque en el segundo caso no sea plana como ya se observó en *Análisis FFT.*

Análisis en el Dominio del Tiempo

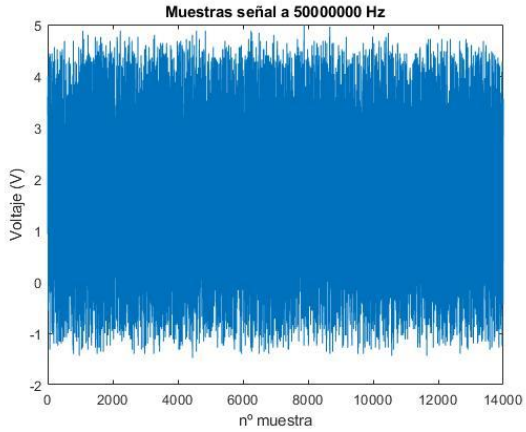


Figura 60: Dominio del Tiempo de la señal muestreada a 50MHz

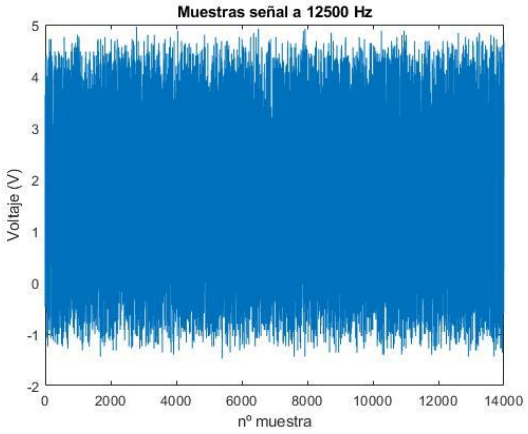


Figura 61: Dominio del Tiempo de la señal muestreada a 12'5kHz

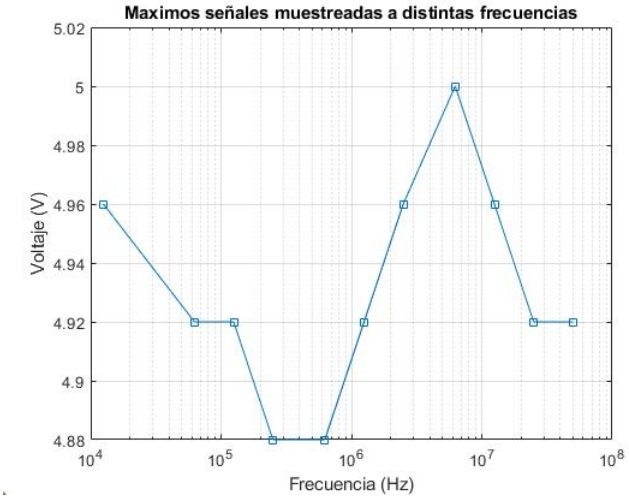


Figura 62: Atenuación en función de la Frecuencia

La Figura 60, Figura 61 y Figura 62, corroboran lo identificado en el apartado anterior sobre el incremento del nivel medio y la atenuación de la señal aleatoria al reducir la frecuencia de análisis (identificado en *6.3.1*). El incremento del nivel medio y la atenuación es debido a la perdida de información al diezmar. Es por ello, que se recomienda muestrear la salida del circuito a la frecuencia a la que se van a analizar los bits posteriormente, evitando cualquier sesgo debido al diezmado.

6.4. MEDIDAS DE LA SALIDA PARA DISTINTOS CIRCUITOS

En esta sección se pretende alcanzar el objetivo principal de este proyecto, adquirir resultados estadísticos fiables realizando las pruebas sobre un gran número de circuitos fabricados por diferentes empresas. De esta forma, se ha estudiado como de sensible es el diseño del circuito ante las tolerancias de cada componente y ante el proceso de fabricación de distintas empresas. Estas medidas son el fruto del conocimiento adquirido durante el desarrollo de las medidas previas, sobre el funcionamiento del circuito y el proceso de postprocesado de las señales.

Se han realizado medidas de entropía y correlación serie sobre 20 circuitos de los 4 fabricantes estudiados, es decir, se han medido un total de 80 circuitos. No se han llegado a medir los 100 circuitos fabricados porque se han tenido que descartar varios de estos circuitos algunos porque directamente no funcionaban, otros por que dejaron de funcionar mientras se median y otros por presentar una salida anómala (añadir figura). El porcentaje de circuitos descartados es del 5%, dos de *Micron20* [48] y uno de *European Circuits* [47], *ShenZhen2U* [49] y *Wurth* [50].

Por último, se han realizado dos tipos de mediciones sobre todos los circuitos: con *enable desactivado*, que se trata del funcionamiento recomendado en [1] y con *enable activado*, haciendo uso del propio bucle de control del boost converter para tener un valor de V_{HIGH} constante de 18V con un pequeño rizado.

6.4.1 MEDICIÓN CON ENABLE DESACTIVADO

Para estas mediciones se ha usado una única frecuencia de muestreo de 125kHz. Se ha escogido esta frecuencia, a pesar de que en *6.3.2* se identificó que la frecuencia óptima de muestreo es 1’25MHz, porque es la más cercana a los 128kHz recomendados en el artículo sin necesidad de diezmar (siguiendo también la recomendación de no diezmar concluida en el punto *6.3.2*). Aun así, cumple con lo definido en *6.3.2* al ser 125kHz una frecuencia válida con espectrograma plano, alta entropía y baja correlación.

El osciloscopio ha capturado las señales en modo *DC* y se ha escogido un nivel para distinguir entre 1 o 0 lógico de 1’65V (la mitad teórica de la señal a la salida del comparador final alimentado entre 0V y 3’3V). Se han muestreado 500 ciclos de *enable on/enable off* (ciclos de 40ms), de los

cuales se han tomado 28ms de la salida aleatoria para el post procesado. Con la frecuencia de muestreo de 125kHz de cada ciclo se han tomado 3500 muestras[6], que suman un total de 1'75M de muestras.

El proceso de muestreo se ha realizado con el script *automatizacion_muestreo_estandar.m*, donde se han capturado los 500 ciclos esperando 1s para muestrear el siguiente ciclo de muestreo. De esta forma nos aseguramos de que no exista correlación entre los datos capturados durante un ciclo y su ciclo anterior o posterior. Para el postprocesado se ha usado el script *procesarDatos.m*, para realizar la conversión a bits y el cálculo de la entropía y la correlación serie. Finalmente, con *plotDatos.m* se han representado las tablas e histogramas que se muestran a continuación.

Análisis Entropía

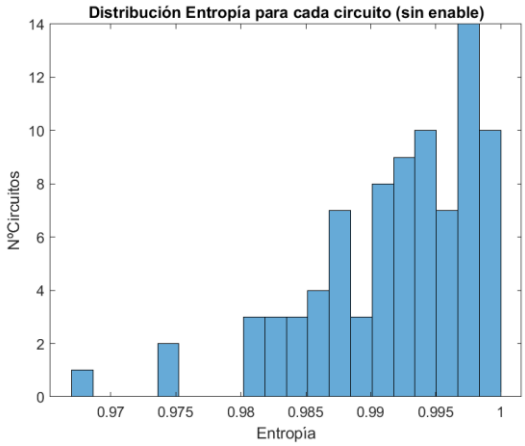


Figura 63: Distribución Entropía sin enable para 80 circuitos

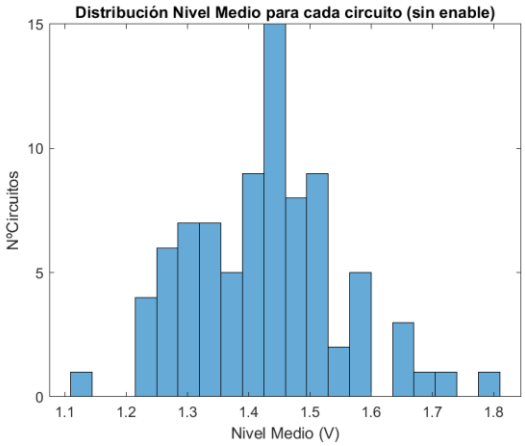


Figura 64: Distribución Nivel Medio sin enable para 80 circuitos

En primer lugar, en la Figura 63 y Figura 64, se muestra la distribución de la entropía y del nivel medio de la salida tomados para 80 circuitos. Se observa como la mayoría de los circuitos presentan entropías elevadas, casi todos por encima de 0'98 (entropía mínima que aseguraban los autores que el circuito generaba). En el caso del nivel medio tiende a seguir una distribución normal exceptuando el gran número de circuitos que presentan un nivel medio de 1'44V. Además, sabemos que la media de los niveles medios es de 1'43V estando por debajo de la esperada de 1'65V. Esto concuerda con las conclusiones de *6.2.3 Medición de las Fuentes del Ruido con Realimentación*, donde se observó

[6] Se ha calculado multiplicando la frecuencia de muestreo (12'5Mz) por el tiempo configurado para capturar bits (28ms).

que la fuente de ruido *NOISE1* y *NOISE2* tienen niveles medios distintos, lo que implica que en el comparador final los niveles medios de las fuentes de ruido no se anulen.

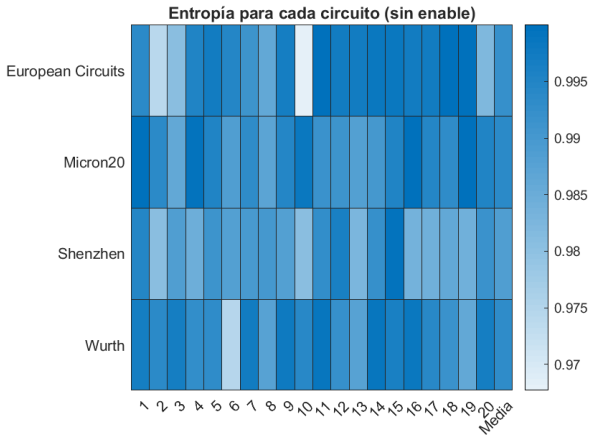


Figura 65: Entropía sin enable para 80 circuitos

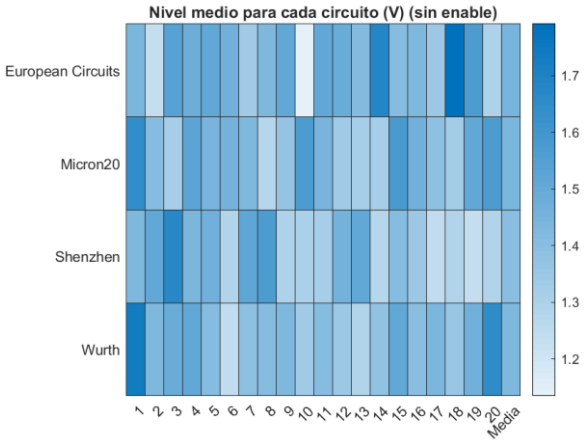


Figura 66: Nivel medio sin enable para 80 circuitos

En la Figura 65, se ha representado la entropía para cada circuito medido agrupándolos por fila según el fabricante al que corresponden. Se puede observar cómo si hay circuitos que destacan por tener una entropía menor (como el 10 de *European Circuits*), pero la mayoría presentan entropías elevadas. En el caso de los de *Shenzhen* la entropía es algo menor, aun así, no se han identificado diferencias significativas entre fabricantes.

En el caso de la Figura 66, se observa como tampoco hay diferencias significativas entre los niveles medios de cada fabricante, aunque haya niveles medios atípicos para algún circuito. Comparando las dos figuras, en el caso del circuito 10 de *European Circuits*, aparte de presentar una entropía baja presenta un nivel medio bajo por lo que se podría argumentar que el decremento de la entropía es debido al nivel medio. Por otro lado, en el circuito 6 de *Wurth*, presenta también una entropía baja, pero, sin embargo, aunque su nivel medio es bajo no difiere del del resto de circuitos. Debido a esto podemos afirmar que el nivel medio del ruido puede llegar a afectar a la entropía de la salida, pero no es el único factor ya que no existe una relación directa para todos los casos. Hay que tener en cuenta otros factores como, por ejemplo, los valores atípicos de las salidas.

Análisis Correlación Serie

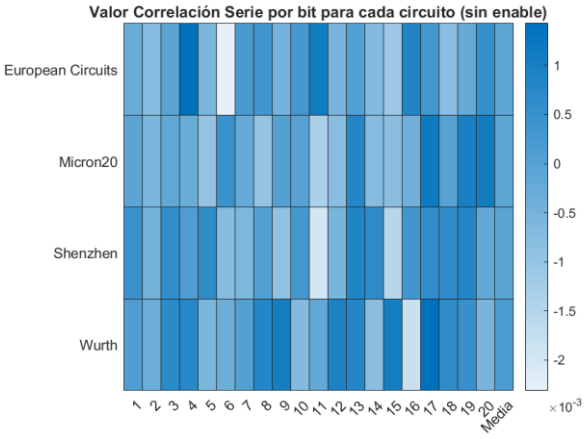


Figura 67: Correlación Serie por bit sin enable para 80 circuitos

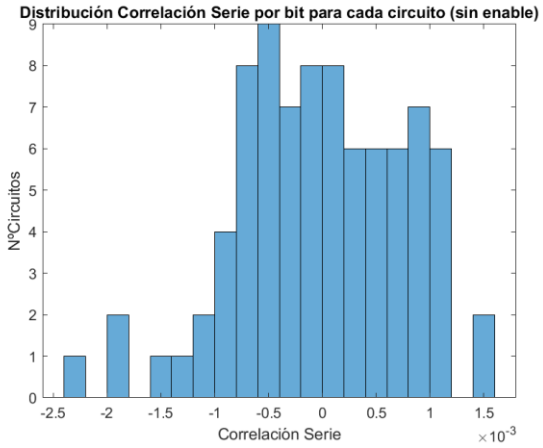


Figura 68: Distribución Correlación Serie por bit sin enable para 80 circuitos

En la Figura 68 se identifica como los valores máximos para la correlación serie por bit son de -0’0025 y 0’0015, lo cual no deja de ser valores muy bajos. La correlación serie por bit media para los 80 circuitos es de -0’00004. También, en la Figura 67 se puede observar cómo, al igual que la entropía, no existen diferencias entre fabricantes y los circuitos con mayores y menores correlaciones encontrándose repartidos entre todos los fabricantes.

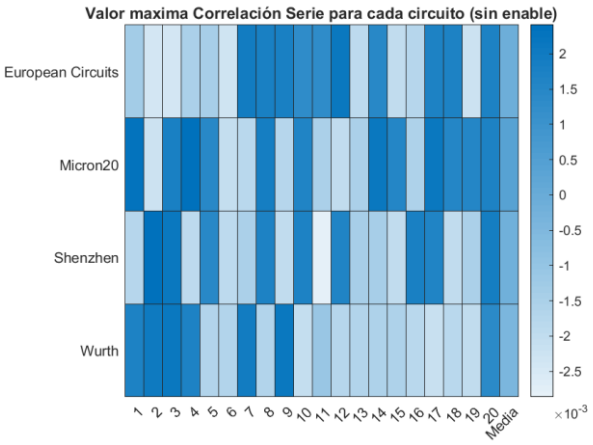


Figura 69: Valor Correlación Serie Máxima sin enable para 80 circuitos

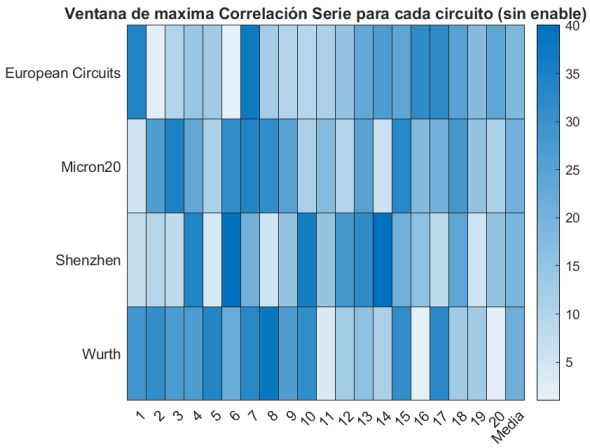


Figura 70: Ventana con la Correlación Serie Máxima sin enable para 80 circuitos

En la Figura 69 se muestra el valor de la máxima correlación serie calculada para ventanas de muestras que van desde 2 (correlación serie por bit) hasta 40. Como se puede observar las correlaciones máximas encontradas siguen siendo muy pequeñas (en torno a ±0’002).

En la Figura 70 se muestra la ventana de muestras para la cual se ha encontrado la correlación serie máxima. En este caso, se puede observar cómo se encuentra bastante distribuida la frecuencia para la cual se detecta una máxima correlación. Además, tampoco existe un sesgo relacionado con el fabricante.

6.4.2 MEDICIÓN CON ENABLE ACTIVADO

La metodología usada para esta medición es la misma descrita en el apartado *6.4.1 Medición con Enable Desactivado*, a excepción del método de adquisición de cada ciclo. En este caso, se han muestreado 500 ciclos de 40ms, pero siempre con el *enable* activado. Esto implica que una vez el *boost converter* alcanza los 18V esta tensión permanecerá constante, ya no existe una fase de carga y otra de descarga en la que la tensión de V_{HIGH} varíe entre 18V y 12V. Para este caso el postprocesado se simplifica al no necesitar muestrear justo durante una ventana concreta de cada ciclo, pues al ser constante la alimentación, se han tomado bits aleatorios durante los 40ms de cada ciclo. Con la frecuencia de muestreo de 125kHz de cada ciclo se han tomado 5000 muestras[7], que suman un total de 2'5M de muestras.

Análisis Entropía

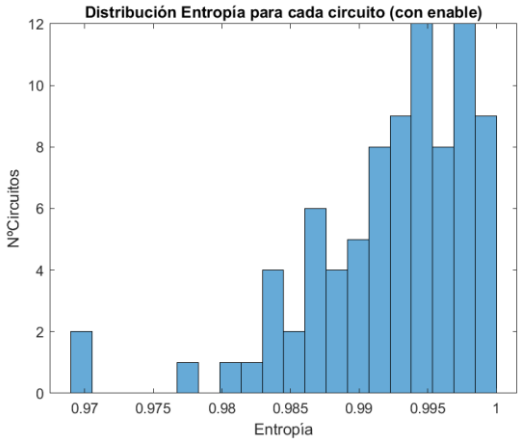


Figura 71: Distribución Entropía con enable para 80 circuitos

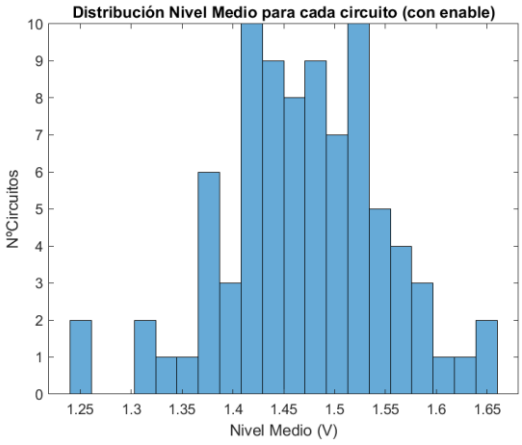


Figura 72: Distribución Nivel Medio con enable para 80 circuitos

Comparando la Figura 71 y Figura 72 con las figuras equivalentes del punto *6.4.1* (Figura 63 y Figura 64), se observa cómo no existen tantos circuitos con un nivel medio de 1'44V. En este caso

[7] En este caso el número de muestras es mayor al pasar de una ventana por ciclo de 28ms a 40ms.

sigue una distribución más similar a una normal. En esta medición la entropía media es de 0'9923 algo mayor que la anterior, de 0'9919. Con el *enable* siempre activado se ha medido también una tensión media de la salida mayor, de 1'47V, lo que puede explicar que la entropía mejore.

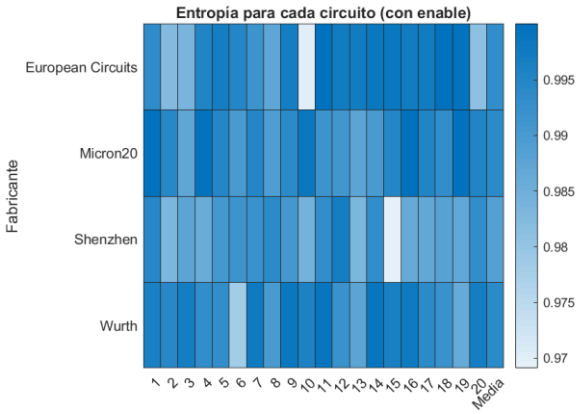


Figura 73: Entropía con enable para 80 circuitos

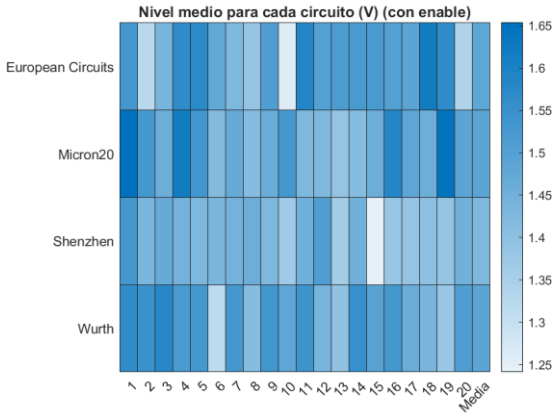


Figura 74: Nivel Medio sin enable para 80 circuitos

Comparando la Figura 73 y Figura 74 con las figuras equivalentes del punto *6.4.1* (Figura 65 y Figura 66), se aprecia como los resultados son también muy similares. En este caso también el 10 de *European Circuits* presenta una entropía significativamente menor que el resto de los circuitos, lo que nos hace pensar que dicha reducción de la entropía no se debe a un error en la ejecución de las medidas, sino que es intrínseco al circuito. Por otro lado, en el caso del circuito 15 de *Shenzhen* tiene una entropía menor a diferencia de lo observado en el punto *6.4.1*. Esto puede ser debido a: imprecisiones en la medida, a que su comportamiento con el enable siempre activado sea peor o simplemente se encuentre dentro de la desviación típica de la salida del circuito.

Análisis Correlación Serie

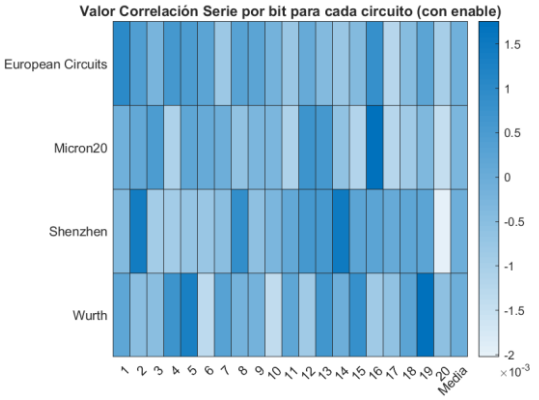


Figura 75: Correlación Serie por bit con enable para 80 circuitos

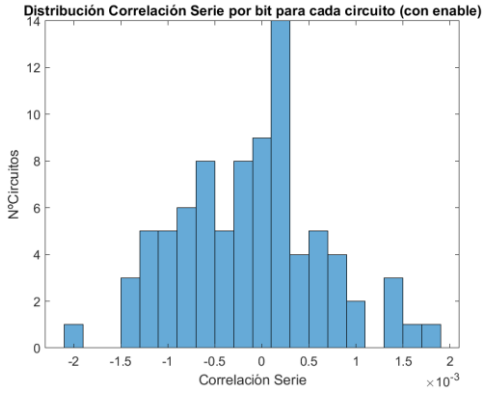


Figura 76: Distribución Correlación Serie por bit con enable para 80 circuitos

En la Figura 75 y Figura 76 se muestra como los resultados obtenidos para la correlación serie por bit son prácticamente idénticos que los del punto *6.4.1*. La única diferencia apreciable es que en Figura 76 hay un gran número de circuitos que presentan una correlación de 0'00025, cosa que no sucede en Figura 68.

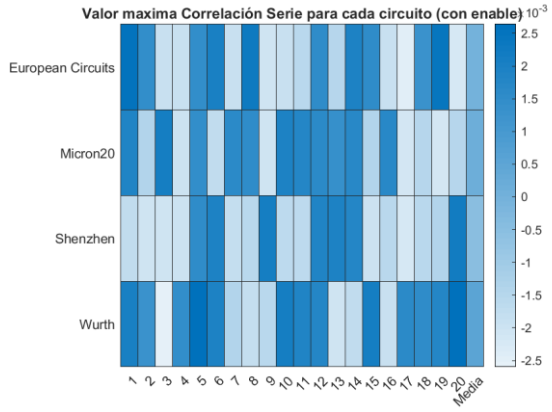


Figura 77: Valor Correlación Serie Máxima con enable para 80 circuitos

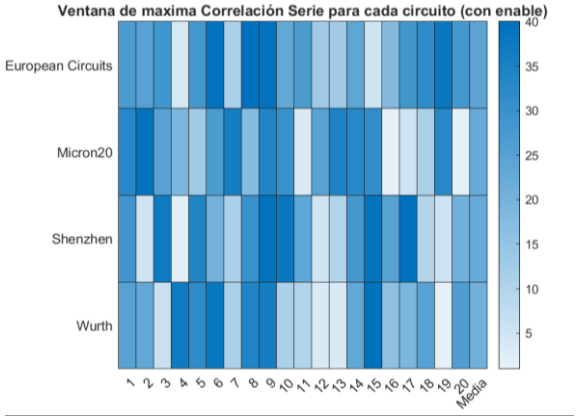


Figura 78: Ventana con la Correlación Serie Máxima con enable para 80 circuitos

En la Figura 77 y Figura 78, al igual que en el punto *6.4.1*, no se ha encontrado un patrón específico para las mediciones de los circuitos de cada fabricante. Además, tampoco existe relación entre las ventanas para la que se ha encontrado la correlación máxima de estas mediciones y las anteriores. Esto nos lleva a pensar que la ventana a la cual se alcanza la máxima correlación serie no es un factor determinístico asociado al circuito. Sin embargo, el rango en el que se sitúan las correlaciones máximas si es el mismo para las dos medidas (de ±0'002).

Capítulo 7. CONCLUSIONES Y TRABAJOS FUTUROS

A continuación, se desarrollan las conclusiones extraídas del análisis del circuito, así como de todas las mediciones experimentales. También se explican las conclusiones generales sobre los RNG, destacando las contribuciones que realiza este estudio, dejando claro qué se han cubierto los objetivos inicialmente establecidos y cuáles son las nuevas líneas de trabajo propuestas.

Conclusiones de las Mediciones

En primer lugar, se han identificado que el *boost converter* descrito en el punto *3.4 Power supply design* de [1] y el implementado para las medidas finales no es el mismo. Nos basamos, por un lado, en que la fase de carga no presenta la misma forma de onda mostrada en [1]. Por el otro, la fase de descarga tiene una duración diez veces menor que la descrita en el artículo. Debido a dichas discrepancias han surgido dudas sobre la justificación realizada en el artículo por la cual recomiendan muestrear únicamente en la fase de descarga.

En segundo lugar, en cuanto al análisis del diodo Zener como generador de ruido, se ha observado como el punto óptimo de máxima generación se produce para un rango reducido de la tensión de alimentación, entre 12’5V y 12’8V. La consecuencia directa de esto es que se necesitaría una fuente de alimentación de precisión para establecer un punto óptimo en cada diodo. En cuanto a la comparación con el artículo los resultados tampoco coinciden, ya que sitúan el punto óptimo en 12’16V.

Finalmente se ha concluido que dicha discrepancia es debida a que no todos los diodos se comportan igual y que cada uno tiene un punto óptimo de trabajo. Dicha conclusión se basa en los resultados de las mediciones presentadas en *6.2.2*, donde se ha medido el ruido generado por 10 diodos distintos. Sería un problema si para cada circuito fabricado hubiera que calcular el punto óptimo de trabajo, pero la realimentación (analizada en *6.2.3*) ayuda a corregir este problema al alcanzar niveles medios similares para circuitos de distintos fabricantes.

Sin embargo, en el punto *6.2.3*, se ha identificado que no se está cumpliendo el principio descrito en el artículo por el cual el nivel medio de las fuentes de ruido debe ser la tensión de referencia en la entrada del bucle. Además, identificamos que los niveles medios de las dos fuentes de ruido son

distintos entre sí, lo que también rompe otro principio descrito en [1], por el cual las dos fuentes de ruido deben tener el mismo nivel medio para que se anulen en la salida y no se vea afectada la entropía de la salida.

En tercer lugar, en el análisis de la frecuencia óptima de muestreo se ha identificado como la máxima recomendable 1’25 MHz, punto en la que el espectro de la señal pasa a ser plano. Para las frecuencias menores, la entropía se encuentra siempre por encima de 0’997 y la correlación serie por debajo de 0’03, valores buenos para conseguir una salida aleatoria. Otra de las conclusiones extraídas de este análisis es la necesidad de evitar el diezmado en el postprocesado, ya que este afecta al nivel medio de las señales además de atenuarlas. Finalmente, es importante destacar la filtración de la señal de un PLC del laboratorio en la salida aleatoria del circuito, ya que si no se corrige podría dar lugar a futuros ataques con el objetivo de reducir la aleatoriedad.

Por último, en cuanto al análisis de la muestra de 80 circuitos y a raíz de las discrepancias en relación con el *boost converter*, se han estudiado dos casos: muestreando solo en la fase de descarga controlada con la señal *enable y* otro en la que el *boost converter* se ha mantenido siempre activado. Una de las conclusiones principales es que no se han encontrado que las medidas con el *enable* siempre activado presenten resultados peores que las medidas únicamente en la fase de descarga. Tampoco se han encontrado sesgos entre los circuitos de cada fabricante, aunque si hay un 3% de los circuitos que presentan una entropía menor y un 5% que venían mal de fabrica o dejaron de funcionar en el desarrollo de las medidas. En líneas generales en este apartado se han obtenido resultados muy similares a los del artículo, con una entropía por encima de 0’97 y una correlación serie por bit menor (en valor absoluto) que ±0’002.

Hay que destacar que el hecho de que estas discrepancias con respecto a lo descrito en el artículo [1] se hayan observado para circuitos de distintos fabricantes, en medidas tomadas en distintos entornos y con configuraciones diferentes, nos permite concluir que se trata de sesgos producidos por la forma en la que está concebido el circuito y no por un problema en la fabricación o en las tolerancias de los componentes.

Conclusiones sobre el Análisis de RNG

En esta memoria se han documentado principalmente los resultados finales desarrollados a lo largo de este año. A pesar de esto, la realización de cada una de las mediciones se ha convertido en

un proceso de ensayo y error, del que se han extraído conclusiones que pueden ser de utilidad para investigadores que auditen circuitos similares al *Lampert Circuit* en un futuro.

En primer lugar, se concluye que uno de los mayores retos del diseño de RNG y en concreto de este estudio es el gran número de ramas de la carrera que se han debido tener en cuenta. Por un lado, las asignaturas de Electrónica más puras para entender el comportamiento de los bucles de realimentación, el funcionamiento de los diodos Zener o el comportamiento de los operacionales, así como para saber manipular adecuadamente la instrumentación del laboratorio. Por otro lado, ha sido de utilidad lo aprendido en la asignatura de *Radiación y Propagación* para entender cómo se estaba propagando el ruido a lo largo del circuito y la importancia de tener en cuenta factores como el largo de las pistas que muchas veces se pasan por alto. Otra de las ramas que se han aplicado son las relacionadas con el Procesamiento de Señales y Teoría de la Comunicación, para poder realizar un postprocesado de las señales correcto. Además, se han necesitado los conocimientos de Estadística para comprender e implementar las pruebas estadísticas de los RNG y recordar conceptos como el de los *p-valor*. Finalmente, ha sido necesario obtener una base sobre criptografía y ciberseguridad para comprender el papel principal que juegan los RNG para conseguir comunicaciones seguras.

En segundo lugar, relacionado con el amplio número de ramas de conocimiento que se ven involucradas, se ha descubierto la complejidad que supone replicar de un estudio sobre un sistema hardware. Si lo contrastamos con el software, es relativamente sencillo preparar el entorno, ejecutar un código disponible en repositorios como GitHub y obtener los resultados casi de inmediato. Sin embargo, en el caso del hardware primero es necesario fabricarlo con las mismas especificaciones, configurar toda la instrumentación necesaria y luego esperar a tomar resultados similares. Dicha complejidad se explica en gran parte debido al gran número de factores que pueden afectar en los resultados finales que los investigadores muchas veces no tienen en cuenta y no se documentan debidamente. De esto último nace una de las principales críticas que se le pueden hacer a [1]: se documenta muy bien el diseño del circuito, pero no se explica apenas como se llevaron a cabo las medidas, la instrumentación usada o las técnicas de postprocesado, así como factores tan fundamentales como el criterio usado para distinguir entre un 1 y un 0 lógico. En consecuencia, se concluye que en base a la experiencia de este trabajo la replicabilidad en hardware es de mayor complejidad que la replicabilidad de sistemas software.

En tercer lugar, se concluye que otra de las críticas que se le pueden hacer al *Lampert Circuit* es la dificultad de su implementación en una aplicación real. Esta afirmación está motivada porque la

salida del circuito es una señal analógica que varía entre 3'3V y 0V, pero que la mayor parte del tiempo se encuentra en valores intermedios (2V-1V). Esto no se puede muestrear directamente con entradas digitales de un procesador o microprocesador, ya que son tensiones para las cuales el fabricante no te asegura si interpretará como un 0 o 1 lógico. Para este estudio ha sido necesario digitalizar la salida con osciloscopio con capacidad de muestrear a altas frecuencias, lo cual lo convierte en una tecnología costosa y que se empotra difícilmente en sistemas criptográficos. En el artículo proponen empotrarlo dentro de un microprocesador usado para el procesamiento de señales de radio de alta frecuencia. Esto sin embargo es difícilmente integrable dentro de un sistema criptográfico o IoT.

Por último, es necesario no sólo destacar los puntos débiles del circuito, sino también sus principales puntos fuertes. Durante el desarrollo del estudio se han podido comparar con otras propuestas de RNG y, dentro de la categoría de RNG basados en fuentes de ruido físicas, el *Lampert Circuit* destaca por la relación entre su sencillez frente a los buenos resultados de entropía y correlación que alcanza. Destaca frente al resto por ser capaz de generar ruido en un amplio rango de frecuencias, no usar ruido de factores externos como la temperatura y la forma en la que usa la realimentación negativa para generar de forma constante ruido. En consecuencia, se considera una buena fuente de RNG que puede tener éxito en el entorno IoT a pesar de que necesita mejorar en algunos aspectos.

Contribuciones y Trabajos Futuros

La principal contribución del trabajo realizado ha sido auditar el *Lampert Circuit*, realizando un análisis riguroso sobre un amplio número de circuitos. Se ha concluido que se trata de un RNG válido para aplicaciones criptográficas IoT pero el cual hay que evolucionar hacia un sistema de fácil implementación y más robusto ante ataques. Además, se ha contribuido facilitando a futuros investigadores la auditabilidad del *Lampert Circuit* para futuras aplicaciones.

Por otro lado, hay que indicar que el fruto de este estudio no se limita únicamente a lo recogido en esta memoria. Los resultados del estudio hasta el momento [60] se presentaron en las *VI Jornadas Nacionales de Investigación en Ciberseguridad* (JNIC) del 2021, congreso científico que recoge las contribuciones dentro del ámbito de la ciberseguridad a nivel nacional. De la presentación del artículo en la JNIC surgió, por parte de los asistentes, especial interés por las posibles vulnerabilidades del circuito y cuestiones sobre la rigurosidad con la que se realizaron las pruebas para analizar la

aleatoriedad. Tras el congreso quedó presente el especial interés por la comunidad científica sobre el *Lampert Circuit* y sobre todo por los RNG en general.

Motivados por lo expuesto en la JNIC y a raíz de las conclusiones de este estudio se plantean tres nuevas líneas de trabajo. La primera es publicar, junto a la documentación del estudio, el código desarrollado en MATLAB para que el resto de los investigadores puedan replicar y auditar este estudio. De este modo se busca iniciar a largo plazo un framework que establezca unas bases y metodología para llevar a cabo el análisis de hardware generador de números aleatorios en particular, y que reduzca la complejidad de la replicabilidad de propuestas basadas en hardware.

La segunda línea de trabajo es continuar las mediciones sobre el circuito buscando posibles vulnerabilidades que puedan invalidar el circuito para aplicaciones criptográficas. Especialmente analizar como de vulnerable es ante ataques de introducción de señale a través de la red eléctrica. En paralelo al análisis de vulnerabilidades es necesario diseñar contramedidas que reduzcan sus efectos, como pueden ser etapas de filtrado que aíslen el circuito de la red.

Finalmente, la tercera línea de trabajo consiste en facilitar la integración del circuito dentro de los sistemas criptográficos, especialmente dentro del entorno de las IoT. Para conseguirlo se plantean, en primer lugar, incorporar una etapa posterior a la salida aleatoria del circuito en la que se digitalice usando un comparador sincronizado con una señal de reloj. Por último, se plantea adaptar el sistema a plataformas como Arduino o Raspberry Pi para que el circuito pueda incorporarse dentro de un gran número de proyectos.

Capítulo 8. BIBLIOGRAFÍA

[1] B. Lampert, R. S. Wahby, S. Leonard and P. Levis, "Robust, low-cost, auditable random number generation for embedded system security," *SenSys '16: Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, pp. 16-27, November 2016.

[2] D. A. Knuth, "vol. 2 Seminumerical Algorithms," in *The Art of Computer Programming (3rd ed.)*, Addison Wesley, 1997-11-14.

[3] L. H. Encinas, La crIptografía, Madrid: CSIC, Los Libros de la Catarata, 2016.

[4] J.-S. Coron, "What is cryptography?," *IEEE Security & Privacy*, vol. 4, no. 1, pp. 70-73, Jan.-Feb. 2006.

[5] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, Oct. 1949.

[6] J. Lan, W. L. Goh, Z. H. Kong and K. S. Yeo, "A random number generator for low power cryptographic application," in *2010 International SoC Design Conference*, Seoul, 2010.

[7] C. Petrie and J. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 5, pp. 615-621, May 2000.

[8] L. Bassham, A. Rukhin, J. Soto, ... and S. Vo, "Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications.," National Institute of Standards & Technology, 2010.

[9] G. Souaki and K. Halim, "Random number generation based on MCU sources for IoT application," *2017 International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, pp. 1-6, 2017.

[10] C. Erbay and S. Ergün, "Random Number Generator Based on Micro-Scale Bio-electrochemical Cell System," in *17th IEEE International New Circuits and Systems Conference (NEWCAS)*, Munich, 2019.

[11] S. Buchovecká, R. Lórencz, F. Kodýtek and J. Bucek, "True Random Number Generator Based on ROPUF Circuit," in *2016 Euromicro Conference on Digital System Design (DSD)*, Limassol, 2016, pp. 519-523.

[12] İ. Taştan and S. Ergün, "A Robust Random Number Generator Based on Chaotic Ring Oscillators," in *2019 17th IEEE International New Circuits and Systems Conference (NEWCAS)*, Munich, Germany, 2019, pp. 1-4.

[13] J. Lan, W. L. Goh, Z. H. Kong and K. S. Yeo, "A random number generator for low power cryptographic application," in *2010 International SoC Design Conference*, Seoul, 2010, pp. 328-331.

[14] J. F. Dynesa, Z. L. Yuanb, A. W. Sharpe and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," *Applied Physics Letters*, vol. 93, no. 3, 2008.

[15] G. Marsaglia, "DIEHARD: A Battery of Tests of Randomness," 1996. [Online]. Available: Link original: http://stat.fsu.edu/pub/diehard/ Disponible en: https://web.archive.org/web/20160125103112/http://stat.fsu.edu/pub/diehard/.

[16] K. H. Tsoi, K. H. Leung and P. H. W. Leong, "Compact FPGA-based true and pseudo random number generators," in *11th Annual IEEE Symposium on Field-Programmable Custom Computing Machines*, Napa, CA, USA, 2003, pp. 51-61, 2003.

[17] C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 5, pp. 615-621, May 2000.

[18] K. Wold and C. H. Tan, "Analysis and Enhancement of Random Number Generator in FPGA Based on Oscillator Rings," in *2008 International Conference on Reconfigurable Computing and FPGAs*, Cancun, 2008, pp. 385-390.

[19] R. G. Brown, D. Eddelbuettel y D. Bauer, «Dieharder: A Random Number Test Suite,» [En línea]. Available: https://webhome.phy.duke.edu/~rgb/General/dieharder.php.

[20] P. L'Ecuyer y R. Simard, «TestU01: A C library for empirical testing of random number generators,» *ACM Transactions on Mathematical Software,* vol. 33, nº 4, August 2007.

[21] A. Lee, M. E. Smid and S. R. Snouffer, "Security Requirements for Cryptographic Modules [includes Change Notices as of 12/3/2002]," Federal Inf. Process. Stds. (NIST FIPS), May 25, 2001.

[22] J. S. Lee, P. Choi, S.-J. Kim, B.-D. Choi y D. K. Kim, «Built-in hardware pseudo-random test module for Physical Unclonable Functions,» *Nonlinear Theory and Its Applications, IEICE,* vol. 5, nº 2, pp. 101-112 , 2014.

[23] National Institute of Standards and Technology (NIST), «Current FIPS,» 23 March 2018 . [En línea]. Available: https://www.nist.gov/itl/current-fips. [Último acceso: 23 Jan 2021].

[24] National Institute of Standards and Technology (NIST), "Random Bit Generation RBG," [Online]. Available: https://csrc.nist.gov/Projects/Random-Bit-Generation. [Accessed 22 Jan 2021].

[25] E. Barker y J. Kelsey, «Recommendation for Random Number Generation Using Deterministic Random Bit Generators,» NIST Special Publication 800-90A Revision 1, June 2015.

[26] E. Barker y J. Kelsey, «Recommendation for Random Bit Generator (RBG) Constructions,» NIST SP 800-90C (Draft), April 2016 .

[27] M. S. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish and M. Boyle, "Recommendation for the Entropy Sources Used for Random Bit Generation," NIST SP 800-90B, January 2018.

[28] L. Ortiz-Martin, P. Picazo-Sanchez y P. Peris-Lopez, «Are the Interpulse Intervals of an ECG signal a good source of entropy? An in-depth entropy analysis based on NIST 800-90B recommendation,» *Future Generation Computer Systems*, vol. 105, pp. 346-360, April 2020.

[29] J. Park, S. Cho, T. Lim, S. Bhunia y M. Tehranipoor, «SCR-QRNG: Side-Channel Resistant Design using Quantum Random Number Generator,» de *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Westminster, CO, USA, 2019, pp. 1-8.

[30] A. Peetermans, V. Rozic y I. Verbauwhede, «A Highly-Portable True Random Number Generator Based on Coherent Sampling,» de *2019 29th International Conference on Field Programmable Logic and Applications (FPL)*, Barcelona, Spain, 2019, pp. 218-224.

[31] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379-423, July 1948.

[32] W. Killmann y W. Schindler, «A proposal for: Functionality classes for random number generators,» 18 Sep 2011.

[33] D. Hurley-Smith, C. Patsakis y J. Hernandez-Castro, «On the unbearable lightness of FIPS 140-2 randomness tests,» *IEEE Transactions on Information Forensics and Security* , April 202.

[34] D. Hurley-Smith y C. H.-C. J. Patsakis, «On the unbearable lightness of FIPS 140-2 randomness tests,» *IEEE Transactions on Information Forensics and Security*, 2020.

[35] V. v. Kaenel y T. Takayanagi, «Dual True Random Number Generators for Cryptographic Applications Embedded on a 200 Million Device Dual CPU SoC,» *2007 IEEE Custom Integrated Circuits Conference*, pp. 269-272, 2007.

[36] Q. H. Dang, «Secure Hash Standard,» *Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology*, Agust 2015.

[37] J. V. Neumann, «Various techniques used in connection with random digits,» *National Bureau of Standards Applied Mathematics Series, page 36-38*, 1951.

[38] H. Zhun y C. Hongyi, «A truly random number generator based on thermal noise,» *ASICON 2001. 2001 4th International Conference on ASIC Proceedings (Cat. No.01TH8549)*, pp. 862-864, 2001.

[39] G. E. Katsoprinakis, M. Polis, A. Tavernarakis, A. T. Dellis y I. K. Kominis, «Quantum random number generator based on spin noise,» *Physical Review A*, 19 May 2008.

[40] S. E. Celal Erbay y T. Kocaeli, «Random Number Generator Based on Micro-Scale,» *2019 17th IEEE International New Circuits and Systems Conference (NEWCAS)*, pp. 1-4, 2019.

[41] R. D. Gavas y R. D. Gavas, «Fast and secure random number generation using low-cost EEG and pseudo random number generator,» *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon),*, pp. 369-374, 2017.

[42] H. Finkelstein, M. J. Hsu y S. C. Esener, «STI-Bounded Single-Photon Avalanche Diode in a Deep-Submicrometer CMOS Technology,» *IEEE Electron Device Letters*, Vols. %1 de %2887-889, p. 27, Nov. 2006.

[43] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti y M. Varanonuovo, «A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC,» *IEEE Transactions on Computers*, vol. 54, pp. 403-409, April 2003.

[44] S. Buchovecká, R. Lórencz, F. Kodýtek y J. Bucek, «True Random Number Generator based on ROPUF,» *2016 Euromicro Conference on Digital System Design (DSD)*, pp. 519-523, 2016 .

[45] J. Holleman, S. Bridges, B. P. Otis y C. Diorio, «A 3 μW CMOS True Random Number Generator With Adaptive Floating-Gate Offset Cancellation,» *IEEE Journal of Solid-State Circuits*, vol. 43, pp. 1324-1336, May 2008.

[46] Tektronix, «TEKVISA CONNECTIVITY SOFTWARE - V4.1.1,» [En línea]. Available: https://www.tek.com/oscilloscope/tds7054-software/tekvisa-connectivity-software-v411. [Último acceso: 9 6 2021].

[47] European Circuits, «https://european-circuits.co.uk/,» [En línea]. Available: https://www.eurocircuits.com/.

[48] Micron20, «https://www.micron20.com/en,» [En línea]. Available: https://www.micron20.com/en.

[49] «ShenZhen2U,» [En línea]. Available: https://www.shenzhen2u.com/.

[50] Würth Industrie Service GmbH & Co. KG, «https://www.wurth.es/,» [En línea]. Available: https://www.wurth.es/.

[51] Test Equipment Solutions, "https://www.testequipmenthq.com/," [Online]. Available: https://www.tek.com/datasheet/tds5032b-tds5052b-tds5054be. [Accessed 16 Nov 2020].

[52] SIGLENT, "https://www.siglenteu.com/power-supplies/spd3303c-series-programmable-dc-power-supply/," [Online]. [Accessed 16 Nov 2020].

[53] RIGNOLA, "https://www.rigolna.com/," [Online]. Available: https://www.rigolna.com/products/waveform-generators/dg1000z/. [Accessed 16 Nov 2020].

[54] B. Lampert, «LampertCircuitRNG GitHub repositorie,» 23 Sep 2019. [En línea]. Available: https://github.com/lampertb/LampertCircuitRNG. [Último acceso: 8 Nov 2020].

[55] Texas Instruments, «TPS6104x Low-Power DC-DC Boost Converter in SOT-23 and WSON Packages datasheet (Rev. J),» [En línea]. Available: https://www.ti.com/product/TPS61041. [Último acceso: 9 Nov 2020].

[56] Semiconductor Components Industries, «MBR0530 Schottky Power Rectifier, Surface Mount,» Dec 2014. [En línea]. Available: http://onsemi.com. [Último acceso: 18 Nov 2020].

[57] Central Semiconductor Corp., «1N746A THRU 1N759A SILICON ZENER DIODES 500mW, 3.3 THRU 12 VOLT, 5% TOLERANCE,» 6 Dec. 2019. [En línea]. Available: https://my.centralsemi.com/get_document.php?cmp=1&mergetype=pd&mergepath=pd&pdf_id=1N746A-759A.PDF.

[58] Texas Instrument, «TLV320x 40-ns, microPOWER, Push-Pull Output Comparators,» Dic 2016. [En línea]. Available: http://www.ti.com/lit/ds/symlink/tlv3202.pdf. [Último acceso: 23 Nov 2020].

[59] Fourmilab, «ENT, A Pseudorandom Number Sequence Test Program,» [En línea]. Available: https://www.fourmilab.ch/random/.

[60] A. Rodríguez, G. López, J. Matanza, C. Rodríguez-Morcillo, Á. López y J. Hernández-Castro, «Análisis y evaluación experimental del circuito generador de números aleatorios Lampert Circuit,» de *VI Jornadas Nacionales de Investigación en Ciberseguridad*, Ciudad Real, España, 9-10 Jun. 2021.

ANEXO I: ALINEACIÓN DEL PROYECTO CON LOS ODS

Si hay uno de los Objetivos de Desarrollo Sostenible (ODS) que pretende alcanzar este estudio es el correspondiente al número nueve, *Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación.* El objetivo 9 promueve una industrialización inclusiva y sostenible de la mano de la innovación y la infraestructura, por lo que generar redes de comunicaciones seguras juega un papel clave. Es capital, basándonos en las últimas tendencias tecnológicas que nos llevan a un mundo más interconectado y accesible, poder desarrollar dicha infraestructura de una forma segura. Es de gran importancia disponer de una infraestructura resiliente, sostenible e innovadora, pero lo es en igual medida que las redes no vulneren los derechos y privacidades de sus usuarios.

A parte del objetivo 9, este estudio contribuye a *Lograr que las ciudades sean más inclusivas seguras, resiliente y sostenibles,* el objetivo ODS número once. Dicho objetivo se centra en el gran incremento que se ha producido en las últimas décadas de los núcleos urbanos. La rápida urbanización lleva muchos casos al surgimiento de barrios pobres, con infraestructuras y servicios insuficientes. Este estudio, en tanto en cuanto contribuye a democratizar el uso de tecnologías básicas para conseguir sistemas criptográficos seguros, puede ser una herramienta de gran utilidad para los nuevos núcleos urbanos. Si se consiguen arquitecturas criptográficas de fácil despliegue y robustas se podrán desplegar ágilmente en estas áreas.

Finalmente, podemos afirmar que otro de los objetivos ODS perseguidos es el 9, sobre *Reducción de las desigualdades*. Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones, consiguiendo prácticamente un acceso universal y asequible para todas las áreas del planeta es una de las metas de este objetivo. Con este estudio se ha contribuido a la investigación de un generador de números aleatorios accesible, de bajo coste y que no requiere de una infraestructura compleja para su uso. Todo ello ayuda a que pueda ser implementado en regiones en desarrollo que no dispongan de dicha infraestructura de manera asequible y fiable, que podría sustituir a sistemas mucho más complejos.