Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE)

Maestría en Ciencias en Electrónica

TRNGs para generación de secuencias muy largas

Autor: Ciro Fabián Bermúdez Márquez

Asesor: Dr. Esteban Tlelo Cuautle (INAOE)
Coasesor: Dr. Cuauhtemoc Mancillas López (CINVESTAV IPN)

18 de mayo de 2023

1. Introducción
2. Objetivos
3. Generadores de números aleatorios (RNGs)
4. Diseño de TRG híbrido
5. Bibliografía

Introducción

Objetivos

Objetivo general

Diseñar e implementar en FPGA un TRNG híbrido para la generación de secuencias muy largas.

Objetivo específicos

- Investigar el estado del arte de diferentes generadores de números aleatorios.
- Estudiar los diferentes tipos de generadores de números aleatorios y analizar sus características principales.
- Estudiar la teoría de los mapas caóticos y su utilidad en generadores de números aleatorios.
- Diseñar un generador de números aleatorios híbrido utilizando un TRNG como generador de semillas y un mapa caótico para realizar un postprocesamiento que mejore sus características estadísticas y comprobar estas utilizando las pruebas NIST.
- Implementar el TRNG híbrido en una FPGA.

Introducción

Estructura de los TRNG

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean lobortis fermentum arcu, in pretium risus convallis vel. Aenean dignissim quis felis.

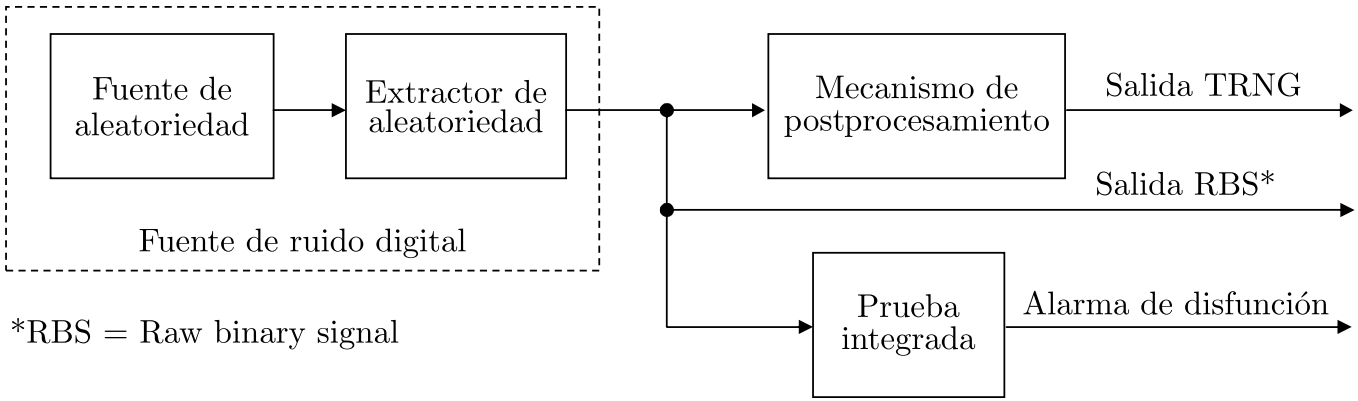


Figura 1: Estructura general de un TRNG [1].

Introducción

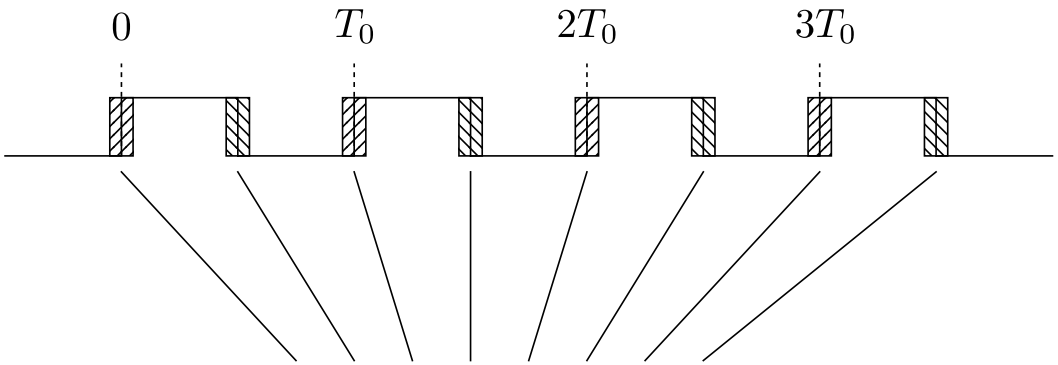
Parámetros de evaluación

- Parámetros relacionados con la calidad
  - Fuente de aleatoriedad.
  - Método de extracción de aleatoriedad y entropía del ruido digital.
  - Método de postprocesamiento (opcional).
  - Tasa de bits de salida y su estabilidad.
- Parámetros relacionados con la seguridad
  - Existencia de un modelo matemático.
  - Comprobabilidad interna.
  - Seguridad (robustez, resistencia contra ataques).
- Parámetros relacionados con el diseño
  - El uso de recursos.
  - El consumo de energía.
  - Viabilidad en dispositivos lógicos y FPGAs.
  - Automatización del diseño.

Introducción

Jitter

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean lobortis fermentum arcu, in pretium risus convallis vel. Aenean dignissim quis felis.



Dependiendo del tamaño del jitter, el flanco de reloj puede llegar en cualquier punto de estas regiones

Figura 2: Jitter del reloj.

Introducción

Jitter

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean lobortis fermentum arcu, in pretium risus convallis vel. Aenean dignissim quis felis.

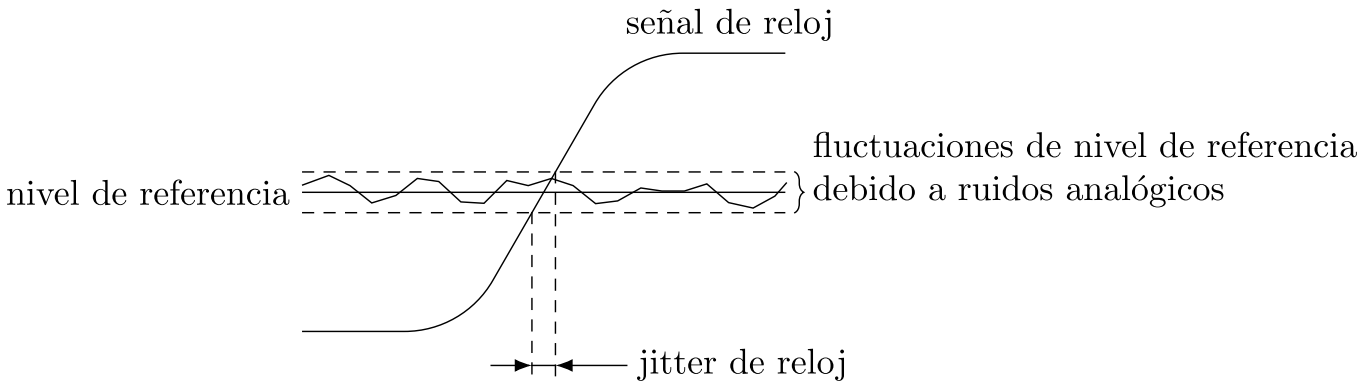


Figura 3: Fluctuaciones del nivel de referencia originadas por ruidos analógicos que provocan jitter del reloj en los circuitos digitales. [2]

Introducción

Núcleos TRNG en FPGA

Con base en los criterios del AIS-20/31 [3], los núcleos TRNG adecuados para utilizarse en dispositivos lógicos programables (FPGA) que usan estructuras oscilantes son:

- Elementary ring oscillator based TRNG (ERO-TRNG).
- Coherent sampling ring oscillator based TRNG (COSO-TRNG).
- Multi-ring oscillator based TRNG (MURO-TRNG).
- Transient effect ring oscillator based TRNG (TERO-TRNG).
- Self-timed ring based TRNG (STR-TRNG).
- Phase-locked loop based TRNG (PLL-TRNG).

Introducción

Núcleo ERO-TRNG

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean lobortis fermentum arcu, in pretium risus convallis vel. Aenean dignissim quis felis interdum aliquam. Duis et vehicula nulla.

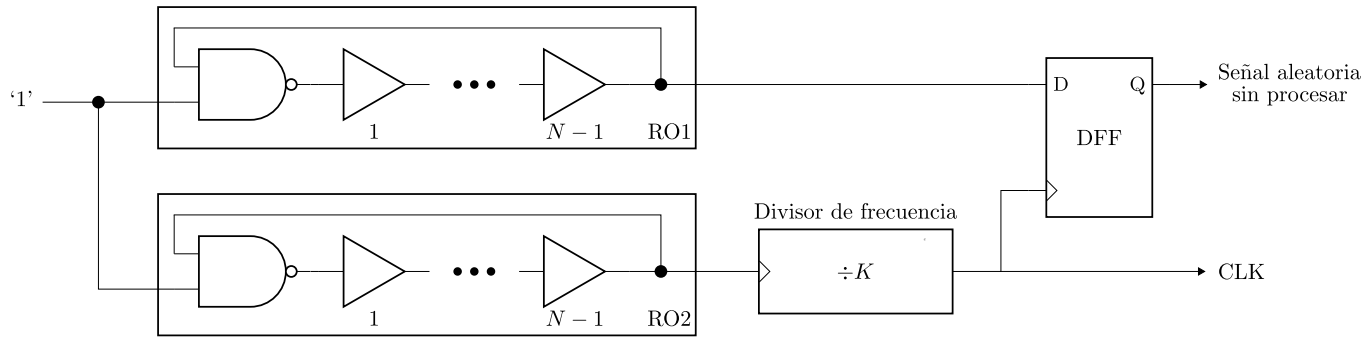


Figura 4: Diagrama de ERO-TRNG.

Introducción

Núcleo COSO-TRNG

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean lobortis fermentum arcu, in pretium risus convallis vel. Aenean dignissim quis felis interdum aliquam. Duis et vehicula nulla.

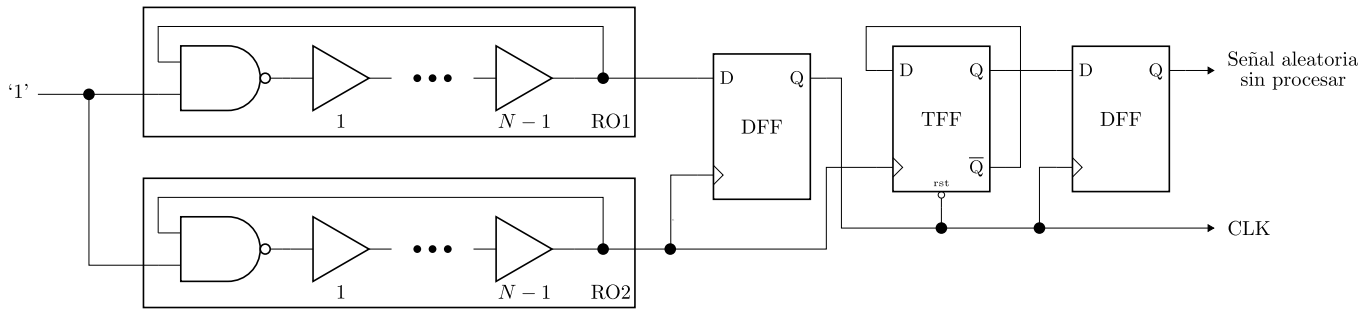


Figura 5: Diagrama de COSO-TRNG.

Introducción

Núcleo MURO-TRNG

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean lobortis fermentum arcu, in pretium risus convallis vel. Aenean dignissim quis felis interdum aliquam. Duis et vehicula nulla.

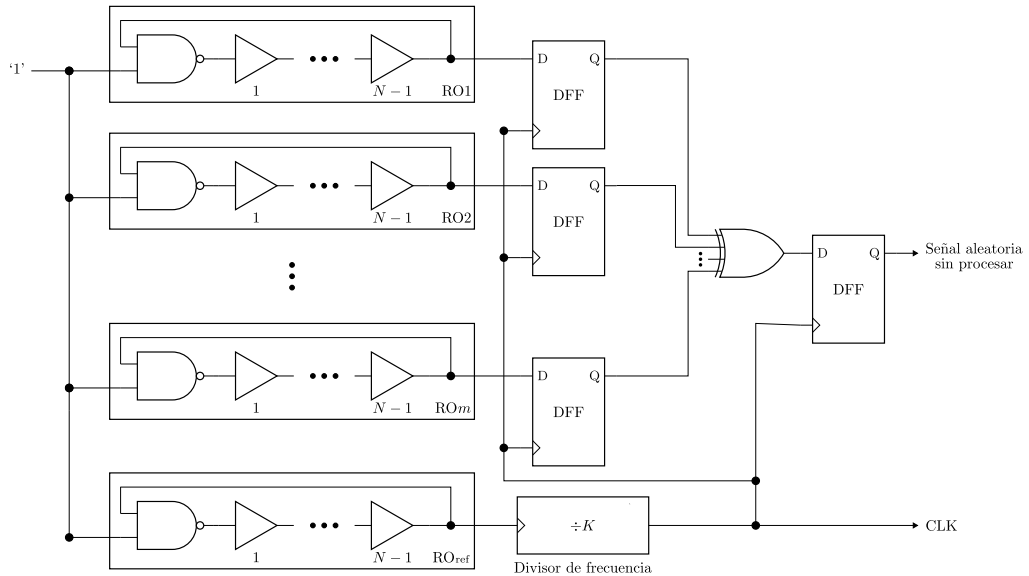


Figura 6: Diagrama de MURO-TRNG.

Introducción

Núcleo TERO-TRNG

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean lobortis fermentum arcu, in pretium risus convallis vel. Aenean dignissim quis felis interdum aliquam. Duis et vehicula nulla.

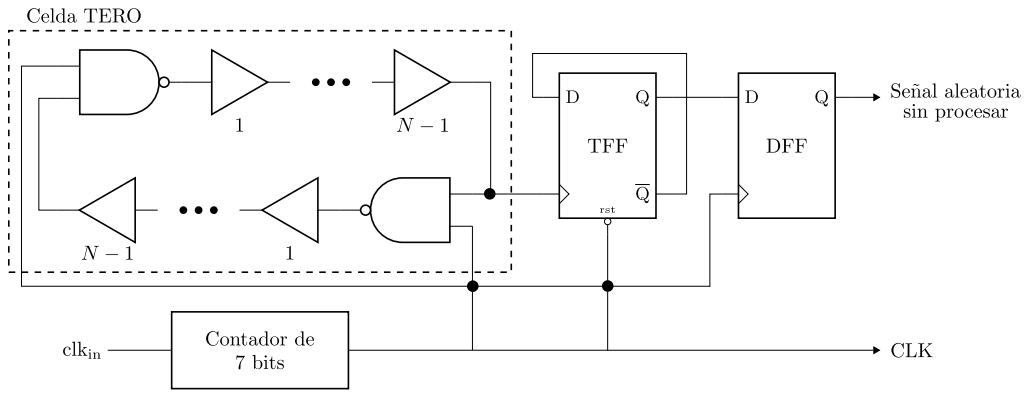


Figura 7: Diagrama de TERO-TRNG.

Introducción

Núcleo STR-TRNG

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean lobortis fermentum arcu, in pretium risus convallis vel. Aenean dignissim quis felis interdum aliquam. Duis et vehicula nulla.

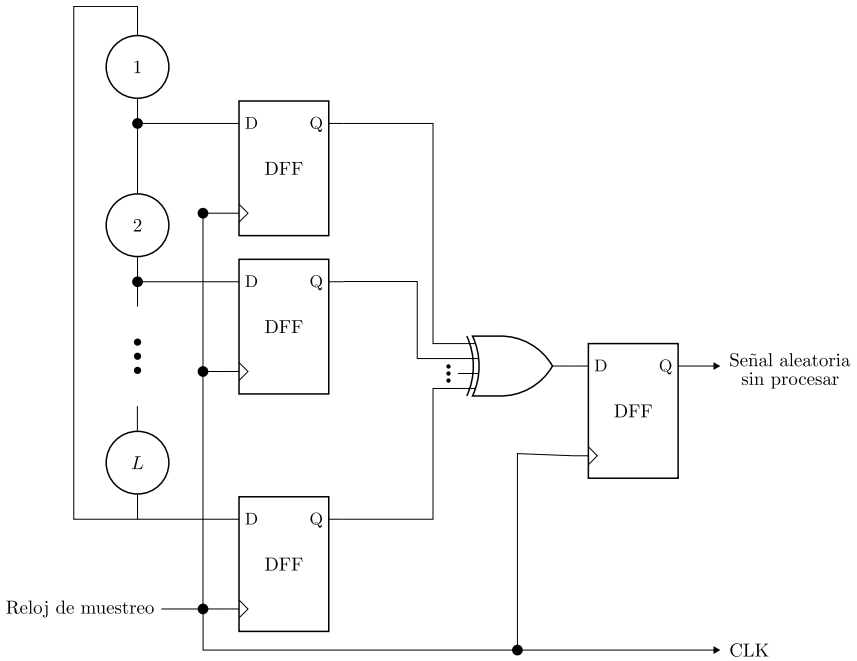


Figura 8: Diagrama de STR-TRNG.

Introducción

Núcleo PLL-TRNG

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean lobortis fermentum arcu, in pretium risus convallis vel. Aenean dignissim quis felis interdum aliquam. Duis et vehicula nulla.

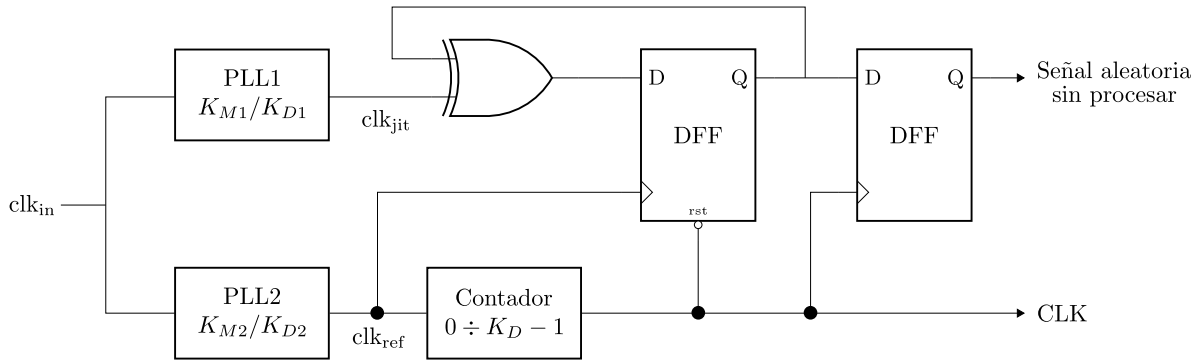


Figura 9: Diagrama de PLL-TRNG.

Introducción

Núcleos TRNG en FPGA

Tabla 1: Resumen de los resultados núcleos TRNGs [3].

TRNG Type	FPGA device	Area (LUT/Reg)	Power cons. [mW]	Bit Rate [Mbits/s]	Efficiency [bits/μWs]	Entropy per bit	Entropy * Bit rate	Feasib. & Repeat.
ERO	Spartan 6	46/19	2.16	0.0042	1.94	0.999	0.004	5
	Cyclone V	34/20	3.24	0.0027	0.83	0.990	0.003	
	SmartFusion 2	45/19	4	0.014	3.5	0.980	0.013	
COSO	Spartan 6	18/3	1.22	0.54	442.6	0.999	0.539	1
	Cyclone V	13/3	0.9	1.44	1600	0.999	1.438	
	SmartFusion 2	23/3	1.94	0.328	169	0.999	0.327	
MURO	Spartan 6	521/131	54.72	2.57	46.9	0.999	2.567	4
	Cyclone V	525/130	34.93	2.2	62.9	0.999	2.197	
	SmartFusion 2	545/130	66.41	3.62	54.5	0.999	3.616	
PLL	Spartan 6	34/14	10.6	0.44	41.5	0.981	0.431	3
	Cyclone V	24/14	23	0.6	43.4	0.986	0.592	
	SmartFusion 2	30/15	19.7	0.37	18.7	0.921	0.340	
TERO	Spartan 6	39/12	3.312	0.625	188.7	0.999	0.624	1
	Cyclone V	46/12	9.36	1	106.8	0.987	0.985	
	SmartFusion 2	46/12	1.23	1	813	0.999	0.999	
STR	Spartan 6	346/256	65.9	154	2343.2	0.998	154.121	2
	Cyclone V	352/256	49.4	245	4959.1	0.999	244.755	
	SmartFusion 2	350/256	82.52	188	2286.7	0.999	188.522	

Título de diapositiva

Título de bloque

$$\begin{aligned} x_{n+1} &= a_1 + a_2 x_n + a_3 x_n^2 + a_4 x_n y_n + a_5 y_n + a_6 y_n^2 \\ y_{n+1} &= a_7 + a_8 x_n + a_9 x_n^2 + a_{10} x_n y_n + a_{11} y_n + a_{12} y_n^2 \end{aligned} \tag{1}$$

Bibliografía

B. Badrignans, J. L. Danger, V. Fischer, G. Gogniat, and L. Torres, eds., *Security Trends for FPGAS*.
Springer Netherlands, 2011.

O. Petura, *True random number generators for cryptography : Design, securing and evaluation*.
Theses, Université de Lyon, Oct. 2019.

O. Petura, U. Mureddu, N. Bochard, V. Fischer, and L. Bossuet, "A survey of AIS-20/31 compliant TRNG cores suitable for FPGA devices," in *2016 26th International Conference on Field Programmable Logic and Applications (FPL)*, IEEE, aug 2016.