Instrumentación de un arreglo de microbolómetros de 120x160

por

Julisa Verdejo Palacios

Tesis presentada en cumplimiento parcial de los requisitos para el grado de:

Maestría en Ciencias en la Especialidad de Electrónica

en

Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE)

Agosto, 2024

Santa María Tonantzintla, Puebla

Asesor:

Dr. Mario Moreno Moreno
Departamento de Electrónica INAOE

Agradecimientos

- Esto es un ejemplo de agradecimiento.
- Este es otro agradecimiento.

Índice general

Índice de figuras

Índice de tablas

Índice de códigos

Resumen

Aqui va un resumen.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Capítulo 1

Introducción

1.1. Estado del arte

Una de las fundamentales a entender cuando se habla de detectores infrarojos es que [1] (pag 34)

Una de las fundamentales a entender cuando se habla de detectores infrarojos es que [1] (pag 60)

Esta es otra cita [2]

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante.

Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

1.2. Objetivos

1.2.1. Objetivo general

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

1.2.2. Objetivos 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.

Capítulo 2

Investigación

2.1. ADCs

2.2. DACs

En este capitulo se presentan los conceptos necesarios para comprender cómo funcionan las diferentes clases de generadores de números aleatorios, sus fuentes de aleatoriedad, sus principales características y cuales son factibles para implementación en FPGA.

El jitter del reloj en un sistema digital es una desviación del flanco de reloj real con respecto a un flanco de reloj ideal. Una señal de reloj ideal se define mediante la ecuación (2.1), donde $t(n)$ representa el tiempo del periodo n-ésimo de una señal de reloj y T es el periodo de una señal de reloj.

$$t(n) = n \cdot T \tag{2.1}$$

En la práctica, una señal de reloj real no alcanza siempre múltiplos enteros de su periodo ideal, sino que sus flancos fluctúan alrededor de este valor debido al jitter. Esta variación es causada por diversos fenómenos físicos, como el ruido térmico, el ruido de la fuente de alimentación y el ruido electromagnético ambiental, entre otros. La Figura 2.1 muestra cómo se ve una señal de reloj afectada por el jitter.

Los parámetros recomendados para configurar las pruebas NIST se muestran en la Tabla 2.1:

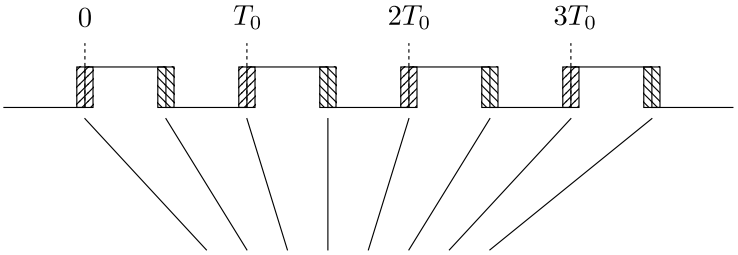

Figura 2.1: Jitter del reloj.

Tabla 2.1: Parámetros recomendados para el conjunto de pruebas del NIST.

Test	**Configuration item**	**Setting**
All tests	Bits per sequence	1000000
All test	Number of sequences (sample size)	1073
Frequency test within a block	Block length	20000
Non-overlapping template test	Template length	10
Overlapping template	Block length	10
Mauler's Universal Statistical test	Test block length L	7
Mauler's Universal Statistical test	Initialization steps	1280
Approximate entropy test	Block length	8
Linear complexity test	Block length	1000
Serial test	Block length	16

Capítulo 3

Mapas caóticos

En este capítulo se estudiarán los mapas caóticos utilizando como ejemplo el mapa logístico para entender cómo produce el caos y las diferentes técnicas para ver de manera cualitativa este fenómeno.

Capítulo 4

Implementación de TRNG híbrido

En este capítulo se describen los pasos para diseñar un mapa caótico y un ERO-TRNG en FPGA para generar bits aleatorios que servirán como semilla a las condiciones del mapa. Se analiza cómo seleccionar el tamaño de palabra de punto fijo utilizando un simulador en C, cómo mejorar el uso de recursos con multiplicadores de una constante y cómo seleccionar el rango valido de la semilla utilizando el dominio de atracción del mapa caótico.

Capítulo 5

Resultados experimentales

En este capítulo se presentan los resultados obtenidos de la implementación del TRNG híbrido, uso de recursos, velocidad de salida y pruebas estadísticas.

Capítulo 6

Conclusiones

- El núcleo ERO-TRNG a pesar de no ser el más rápido de los generadores que se pueden implementar dentro de las FPGA, tiene muy buena entropía, un modelo estocástico muy bien estudiado, una metodología de diseño bien estructurada y por lo mismo es fácil de implementarse no requiriendo intervención manual en la colocación de los componentes dentro del FPGA. Debido a lo anterior fue perfecto para generar semillas, una vez obtenida la semilla la velocidad del sistema ya no depende del ERO-TRNG lo que contrarresta su desventaja principal. Su repetibilidad en diferentes familias de FPGA, la seguridad que agrega al generador y la pequeña cantidad de recursos que requiere son las ventajas que presentó este núcleo.

- El mapa caótico bidimensional que se seleccionó para este trabajo es muy flexible, ya que se tiene 12 parámetros diferentes para configurarse, lo que se ve reflejado en diferentes atractores que pueden utilizarse para generar secuencias de bits aleatorias. Mientras las condiciones iniciales del atractor se encuentren dentro del dominio de atracción de este, podemos sembrar el mapa sin problemas.

- La implementación del TRNG híbrido utiliza un 88 % de los DPS y tan solo un 7 % de los LUTs de la FPGA, no obstante considerando que la FPGA utilizada es de bajos recursos, para FPGAs más grandes las cuales tienen de 4 a 5 recursos, este sistema no representa un gran consumo de área.

- El TRNG híbrido que se diseño en este trabajo pasó todas las pruebas NIST y el análisis estadístico demostró distribuciones uniformes, además debido a que en su núcleo se encuentra un TRNG que pasa todas las pruebas de la AIS20/31 la seguridad del sistema se ve garantizada mientras nadie tenga acceso a la semilla.

- La velocidad obtenida por el TRNG híbrido fue de 533.33 Mbit/s, es ligeramente superior a sistemas similares las cuales rondan los 400 Mbit/s.

Apéndice A

Códigos

A.1. Códigos de Verilog

Código A.1: Comunicación RS232

```
%% prog04_graficas_multiples
clear; close all; clc;
x = 0:0.1:2*pi;
y1 = sin(x); y2 = cos(x);

subplot(2,1,1);
plot(x,y1,'-sr','DisplayName', 'f(x) = sin(x)');
axis( [min(x) max(x) min(y1)*1.1 max(y1)*1.1] );
grid on; grid minor;
legend('Location','northeast','FontSize', 12);
title('f(x) = sin(x)'); xlabel('x'); ylabel('f(x)');

subplot(2,1,2);
plot(x,y2,'-sk','DisplayName', 'f(x) = cos(x)');
axis( [min(x) max(x) min(y2)*1.1 max(y2)*1.1] );
grid on; grid minor;
legend('Location','southeast','FontSize', 12);
title('f(x) = cos(x)');  xlabel('x'); ylabel('f(x)');
```

A.2. Códigos de Verilog

Código A.2: Máquina de estados ejemplo.

```
module counter #(
  parameter Width = 8
) (
  input              clk_i,
  input              rst_i,
  output             max_tick_i,
  output [Width-1:0] q_o
);

  reg  [Width-1:0] reg_q;
  wire [Width-1:0] sum_d;

  assign sum_d = reg_q + 1;
  assign max_tick_i = (reg_q == 2**Width-1) ? 1'b1 : 1'b0;

  always @(posedge clk_i, posedge rst_i) begin
    if (rst_i)
      reg_q <= 0;
    else
      reg_q <= sum_d;
  end

  assign q_o = reg_q;

endmodule
```

Bibliografía

[1] A. Rogalski, *Infrared Detectors*. Taylor and Francis Group, 2020.

[2] X. He, G. Karunasiri, T. Mei, W. Zeng, P. Neuzil, and U. Sridhar, "Performance of microbolometer focal plane arrays under varying pressure," *IEEE Electron Device Letters*, vol. 21, pp. 233–235, may 2000.