CACiC 2023
CONGRESO ARGENTINO DE CIENCIAS DE LA COMPUTACIÓN

Generador Binario Pseudoaleatorio Basado en la Combinación de Registros de Desplazamiento de Retroalimentación Lineal con Función de Filtrado No Lineal

Andrés Francisco Farías – Andrés Alejandro Farías

Departamento Académico de Ciencias Físicas, Matemáticas y Naturales
Universidad Nacional de La Rioja, La Rioja. Argentina
afarias665@yahoo.com.ar, andres_af86@hotmail.com

Abstract. Este trabajo desarrolla el procedimiento para la construcción de un generador binario pseudoaleatorio basado en la combinación mediante función por mayoría de registros de desplazamiento con retroalimentación no lineal (Linear Feedback Shift Register, LFSR).

El proceso incluye: características de los LFSR, definición del modelo, elección de los distintos LFSR, selección de funciones booleanas en base a sus óptimas propiedades criptográficas, composición del generador con los componentes seleccionados, clave y el procedimiento para generarlas, elección de las pruebas estadísticas a utilizar y los criterios de análisis de los resultados, puesta en funcionamiento y realización de las pruebas de aleatoriedad necesarias sobre las secuencias obtenidas.

Keywords: LFSR, generator, key, boolean function, non-linearity.

1. Introducción

Los generadores binarios pseudoaleatorios deben entregar secuencias de calidad y además se les exige imprevisibilidad y facilidad de implementación, pero, fundamentalmente un período con una longitud significativa.

Es en esos términos que se propone un modelo que responda a tales exigencias. La modalidad elegida se basa en la combinación no lineal de generadores conformados por ocho NLFSR, que tienen una función booleana de filtrado [1], [2].

El procedimiento de construcción de un generador pseudoaleatorio de ese estilo requiere de varias etapas:

- Características de los LFSR
- Definición del modelo.
- Elección de los distintos LFSR, base del sistema.
- Selección de funciones booleanas de cuatro variables en base a sus óptimas propiedades criptográficas.
- Composición del generador con los componentes ya seleccionados.
- Clave y el procedimiento para generar los estados iniciales de los LFSR.
- Elección de las pruebas estadísticas a utilizar y los criterios de análisis de los resultados.

- Puesta en funcionamiento y realización de las pruebas de aleatoriedad necesarias sobre las secuencias obtenidas. Generador binario pseudoaleatorio

1.1 Características de los LFSR

Los LFSR que se utilizan tienen la siguiente estructura:

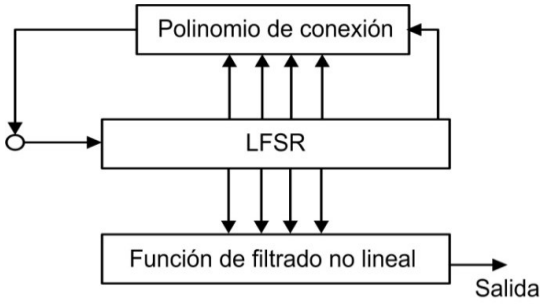

Fig. 1. Esquema del LFSR

1.2 Definición esquemática del modelo

El generador propuesto en este trabajo, está conformado por cuatro LFSR, que tienen cada uno, una función booleana de filtrado no lineal, que producen secuencias binarias, las que luego son combinadas mediante otras funciones booleanas de combinación, y una operación final XOR, según la figura 2:

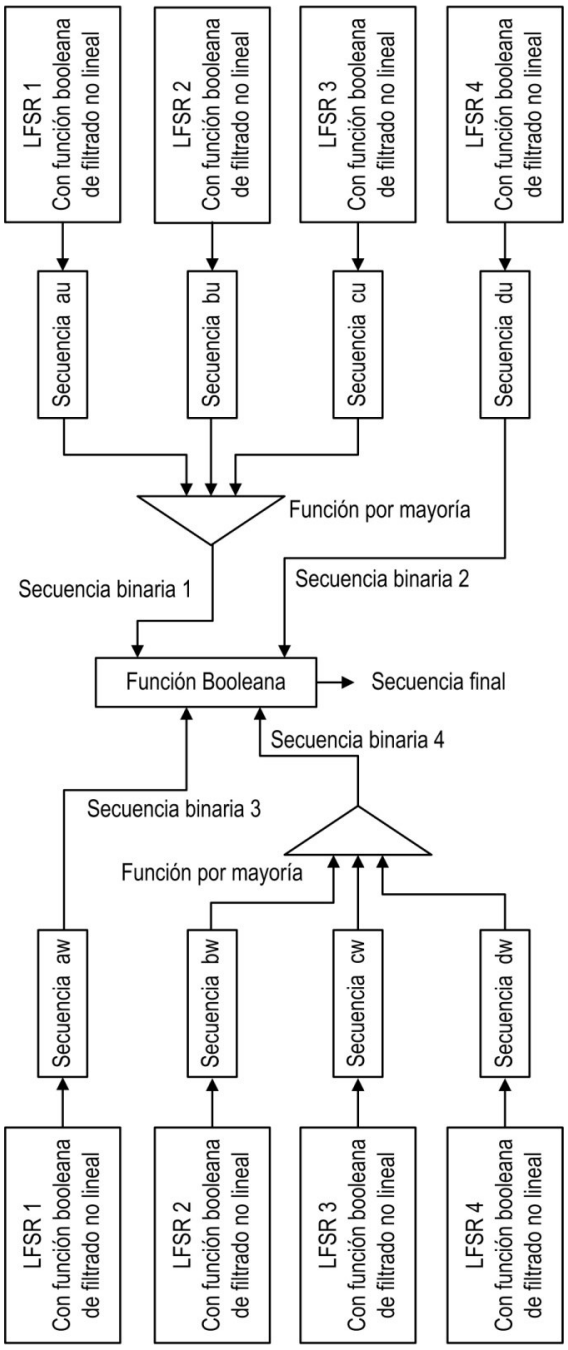

Fig. 2. Esquema generador binario pseudoaleatorio

1.3 Elección de los distintos LFSR

Las longitudes y polinomios primitivos de cada LFSR, que componen el generador, son las siguientes [3], [4], [5], en la tabla 1 y en la figura 2 se indican como queda el dispositivo.

Tabla 7. LFSR, longitudes y polinomios primitivos del Generador

LFSR	Longitud	Polinomios primitivos
2	41	$P(x)_3 = x^{41} + x^{32} + x^{31} + x^{27} + 1$
3	43	$P(x)_4 = x^{43} + x^{27} + x^{22} + x^5 + 1$
3	59	$P(x) = x^{59} + x^{54} + x^{46} + x^{26} + 1$
4	53	$P(x) = x^{53} + x^{50} + x^{41} + x^{20} + 1$

1.4 Selección de las funciones booleanas

Propiedades criptográficas deseables.

A continuación, se indican algunas de las propiedades criptográficamente más significativas, adoptadas para este trabajo [6], [7], [8].

- **Función Balanceada:**
- **No Linealidad**:
- **Grado Algebraico**:
- **Criterio de Avalancha Estricto**

Siguiendo los criterios arriba indicados las funciones booleanas aceptadas, son observadas en tabla 2:

Taba 8. Funciones de cuatro variables adoptadas

f_{NAF}	No linealidad	Cumple SAC
$f_{84} = a \cdot c \oplus b \cdot c \oplus a \cdot d \oplus b \cdot d \oplus c \cdot d$	4	Sí
$f_{89} = a \cdot c \oplus b \cdot c \oplus d \oplus a \cdot d \oplus b \cdot d$	4	Sí
$f_{100} = a \cdot c \oplus b \cdot c \oplus d \oplus a \cdot b \cdot d \oplus c \cdot d$	4	Sí
$f_{176} = c \oplus a \cdot c \oplus b \cdot c \oplus a \cdot d \oplus b \cdot d$	4	Sí
$f_{199} = c \oplus a \cdot c \oplus b \cdot c \oplus d \oplus c \cdot d$	4	Sí
$f_{381} = c \oplus a \cdot b \cdot c \oplus a \cdot d \oplus b \cdot d \oplus c \cdot d$	4	Sí
$f_{468} = c \oplus d \oplus a \cdot d \oplus b \cdot d \oplus c \cdot d$	4	Sí
$f_{536} = a \cdot b \oplus b \cdot c \oplus a \cdot d \oplus b \cdot d \oplus c \cdot d$	4	Sí
$f_{5056} = a \oplus b \oplus a \cdot d \oplus b \cdot d \oplus c \cdot d$	4	Sí

1.5 Conformación del generador combinacional

El generador combinacional se indica en la figura 3:

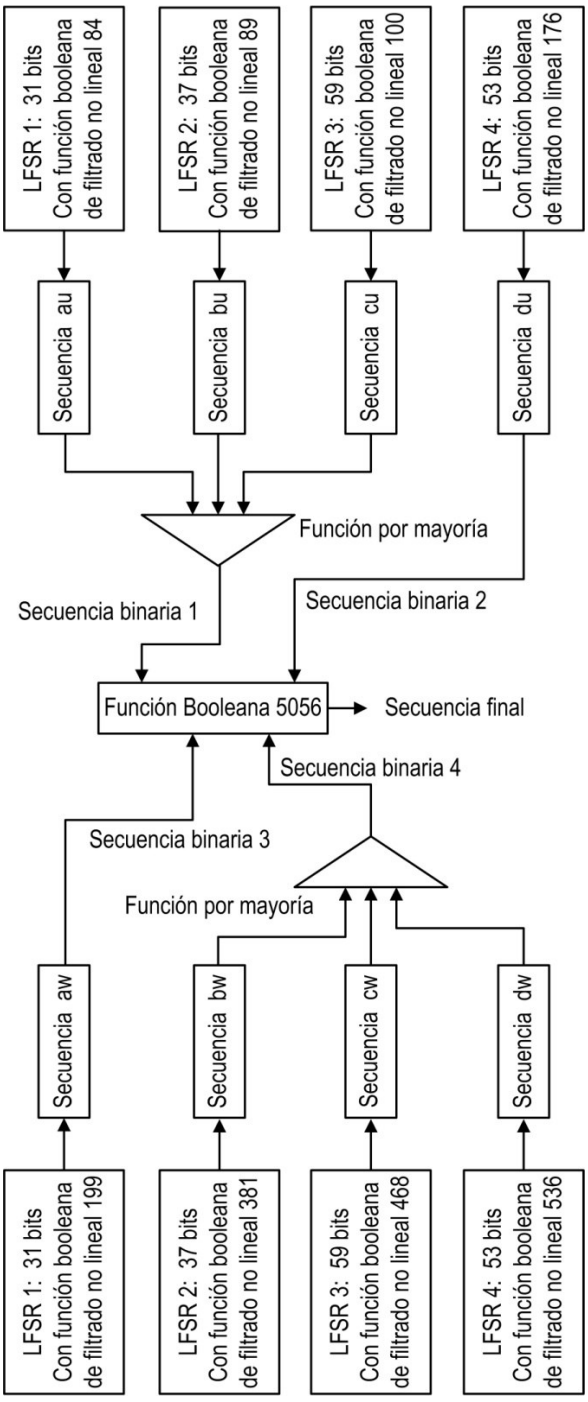

Fig. 3. Generador Combinacional

1.6 Clave

Para originar los estados iniciales de los distintos LFSR se realiza un proceso que utiliza una clave de 32 caracteres, que expresada en código ASCII (American Standard Code for Information Interchange), tiene longitud de 256 bits.

La clave es sometida a un proceso criptográfico, que se indica en la figura 4.

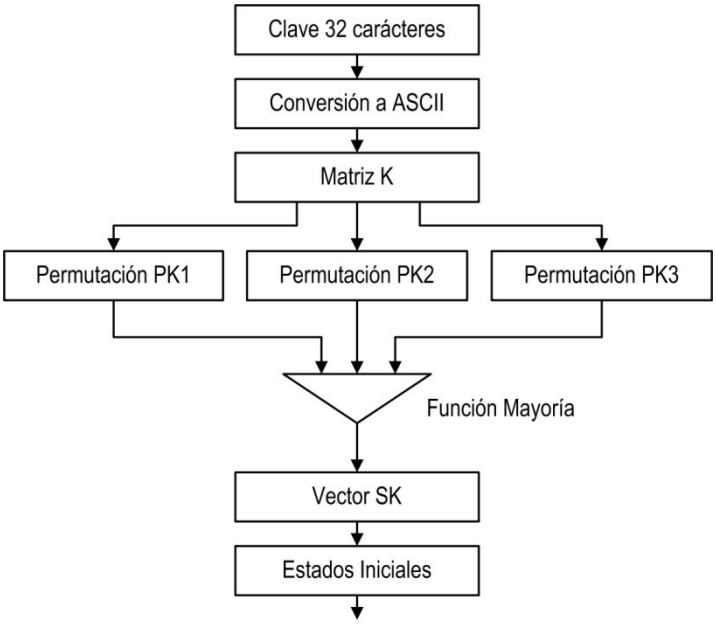

Fig. 4. Clave para el generador

1.7 Permutaciones

Generador congruencial multiplicativo: El generador tiene la siguiente expresión: [9]

$$x_{i+1} = (a_x \cdot x_i)mod\ m_x \qquad (4)$$

Donde:

$$a_x = multiplicador$$
$$m_x = módulo$$
$$x_0 = semilla$$

Tabla.3. Vectores, módulos, multiplicadores y semillas

Vector	módulo	multiplicador	semilla
PK1	1048576	1747	3249
PK2	1048576	1753	3271
PK3	1048576	1759	3301

De la operación resulta un vector SK[j] de 256 bits, que es el que proveerá los estados iniciales de los LFSR, en forma secuencial.

2. Pruebas de aleatoriedad

2.1 Elección de las pruebas estadísticas

Fueron seleccionadas algunas pruebas de la Norma NIST Special Publication 800-22, del trabajo de Rukhin (et al.) [10].

- Prueba de frecuencia
- Prueba de frecuencia en un bloque
- Prueba de rachas
- Prueba de rachas de unos en un bloque
- Prueba de sumas acumuladas
- Prueba de entropía aproximada

2.2 Pruebas sobre el generador

Se analizaron cien secuencias binarias de 100.000 bits, obtenidas del generador a partir de cien claves distintas. El nivel de significancia adoptado para las pruebas estadísticas es de $\alpha = 0{,}01$. La hipótesis nula es:

$$H_0 \rightarrow \text{p\_valor} > 0{,}01$$

2.3 Proporción de muestras que pasan las pruebas

Para el análisis de los resultados, se determina la proporción de muestras que superan las pruebas, y con esos datos se construye un gráfico de puntos, luego se verifica si los mismos caen dentro de los límites superior e inferior, donde k es el número de muestras. $LS, LI = (1-\alpha) \pm 3 \cdot \sqrt{\alpha \cdot (1-\alpha)/k}$

En nuestro caso $k = 100$ y el nivel de significancia elegido es: $\alpha = 0.01$, los límites quedan: $LS = 1{,}02$ y $LI = 0{,}96$

Se consideran todas pruebas, los resultados se indican en la tabla 4.

Table 9. Pruebas estadísticas

Pruebas	Proporción	Superior	Inferior
Frecuencias	1,00	1,02	0,96
Frecuencias en un Bloque	0,97	1,02	0,96
Rachas	1,00	1,02	0,96
Rachas de Unos en un Bloque	0,98	1,02	0,96
Sumas Acumuladas Adelante	1,00	1,02	0,96
Sumas Acumuladas Atrás	0,97	1,02	0,96
Entropía Aproximada	1,00	1,02	0,96

En la figura 5 se aprecia el resultado, en definitiva, las secuencias que entrega el generador superan las pruebas de aleatoriedad.

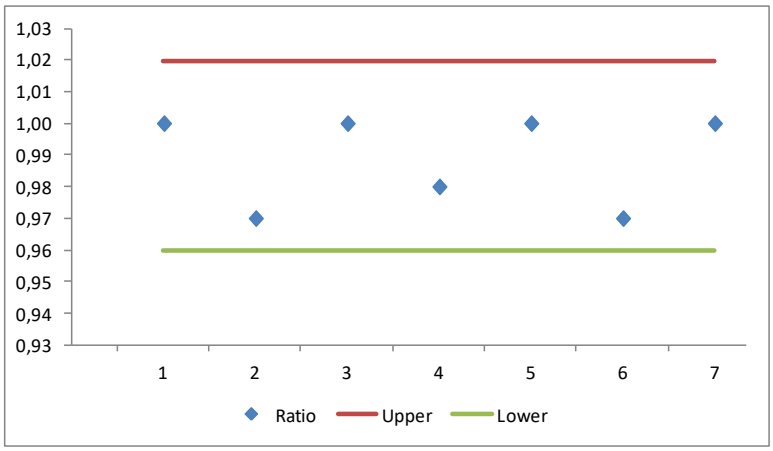

Fig. 5. Gráfico de puntos

3. Conclusiones

Se diseñó un dispositivo que combina en forma no lineal las secuencias producidas por ocho generadores compuestos por LFSR con funciones paralelas de filtrado. Para se dispuso del auxilio de la función por mayoría, junto con una función booleana final de cuatro variables.

Los NLFSR que componen cada generador tienen polinomios de conexión primitivos, lo que asegura un elevado período en la secuencia resultante.

Las funciones booleanas son las responsables del proceso no lineal y aseguran las mejores prestaciones criptográficas. Realizado el proceso de selección, las funciones fueron incorporadas al generador y luego puestas a funcionar para generar las secuencias respectivas con distintos valores de claves y ser sometidas a las pruebas de aleatoriedad.

Los resultados obtenidos fueron satisfactorios, por lo que el modelo presentado se considera válido para la generación de secuencias pseudoaleatorias de buena calidad criptográfica.

Referencias

1. Massodi, F., Alam, S. and Bokhari, M., “A Analysis of Linear Feedback Shift Registers in Stream Ciphers”, International Journal of Computer Application, 16 (17), pp. 0975 – 887, 2012.
2. Menezes, A.,Van Oorschot, P. and Vanstone, S., “Handbook of Applied Cryptography”, Massachusetts Institute of Technology, 1996.
3. Parr, C. and Pelzl, L., Understanding Cryptography, Springer, 2010.

4. Stahnke, W., "Primitive Binary Polynomials", Mathematics of Computation, 27. 124, pp. 977-980, 1973.
5. Seroussi, G., "Table of Low-Weight Binary Irreducible Polynomials", Computer Systems Laboratory, 1998.
6. Clark, J., Jacob, J., Maitra, S., Stanica, P.: Almost Boolean Functions: The Design of Boolean Functions by Spectral Inversion. Computational intelligence. 20. (3), 450—462 (2004)
7. Braeken, A.: Cryptographic Properties of Boolean Functions and S-Boxes. Faculteit Ingenieurswetenschappen. Katholieke Universiteit Leuven (2003)
8. Elhosary, A., Hamdy, N., Farag, I., Rohiem, I.: State of the Art in Boolean Functions Cryptographic Assessment. International Journal of Computer Networks and Communications Security.1. (3), 88--94 (2013)
9. Fishman, G.: Multiplicative Congruential Random Number Generators with Modulus 2ß : An Exhaustive Analysis for ß = 32 and a Partial Analysis for ß = 48. Mathematics of Computation. 54. (189), 33--344 (1990)
10. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., and Vo, S., "A Statistical Prueba Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", National Institute of Standards and Technology, (2000).