

# Operación XOR de manera cruzada en mapas Renyi donde $i \neq j$ , aplicación de pruebas NIST.

Marcos Daniel Calderón Calderón  
Maestría en Ciencias de la Computación  
Centro de Investigación en Matemáticas (CIMAT)  
Guanajuato, Gto.  
marcos.calderon@cimat.mx

**Resumen**—En este reporte se explica de manera detallada el funcionamiento de una operación XOR de manera cruzada entre la parte inferior y superior de dos números por mapas caóticos Renyi. Pero ahora se tiene la restricción de que el valor de  $i$  sea diferente del valor de  $j$ .

## I. INTRODUCCIÓN.

EL mapa caótico Renyi tiene la siguiente forma:

$$f(k) = \left( q2^{n-i}k + \left\lfloor \frac{k}{2^j} \right\rfloor \right) \text{ mód } 2^n \quad (1)$$

El esquema que se para su combinación es el siguiente:

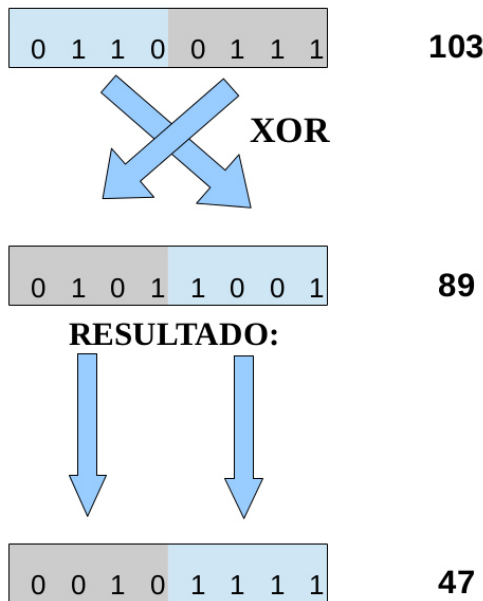


Figura 1. Esquema de intercambio.

Ahora, para los ejemplos que se muestran aquí se utilizan 32 bits, esto significa que se van a dividir los datos generados por los mapas caóticos en dos partes: cada una de 16 bits.

También, en este caso, necesitamos un nuevo valor para  $a$ :  
( $a = 2^{16} - 1 = 65,535$ )

## II. EJEMPLO 1.

### II-A. Procedimiento.

Para este ejemplo, se han elegido los siguientes valores:

- Mapa 1:  $i = 5$   $j = 7$ .
- Mapa 2:  $i = 6$   $j = 14$ .

Ahora, es necesario elegir un valor de  $q$  adecuado, en este ejemplo, utilizamos los siguientes:

- Mapa 1:  $q = 13$ .
- Mapa 2:  $q = 19$ .

Ahora, es necesario calcular el parámetro que se forma de la expresión:

$$\beta = q2^{n-i} \quad (2)$$

con base en lo anterior, se encontraron los siguientes parámetros para el mapa 1 y el mapa 2 respectivamente:

- $\beta_1 = 1744830464$ .
- $\beta_2 = 1275068416$ .

También es importante elegir el tipo de dato que se va a utilizar para almacenar los valores generados por los mapas, en este caso se eligió el tipo de dato **unsigned long** (se utilizó un equipo con arquitectura de 32 bits, donde este tipo de dato tiene un tamaño de 32 bits).

Se generaron 80,000 valores a la hora de relacionar los valores de los dos mapas con la operación XOR. Como cada valor está formado de 32 bits, se obtiene un total de 2,560,000 bits para la aplicación de pruebas NIST.

Se utilizó el siguiente código para la ejecución de las pruebas NIST:

- **./assess 2560000**
- User Prescribed Input File: **dosRenyisIntercambio1difj.dat**
- Enter 0 if you DO NOT want to apply all of the statistical tests to each sequence and 1 if you DO. Enter choice: **1**
- How many bitstreams? **1**
- Input File Format: [0] ASCII - A sequence of ASCII 0's and 1's [1] Binary - Each byte in data file contains 8 bits of data
- Select input mode: **1**

## II-B. Resultados.

Los resultados no son buenos, de hecho ninguna prueba es aprobada.

## III. EJEMPLO 2.

### III-A. Procedimiento.

Para el ejemplo 2, se eligieron los siguientes parámetros:

- Mapa 1:  $i = 8$   $j = 13$ .
- Mapa 2:  $i = 10, j = 15$ .

Ahora, es necesario elegir un valor de  $q$  adecuado, en este ejemplo, utilizamos los siguientes:

- Mapa 1:  $q = 29$ .
- Mapa 2:  $q = 31$ .

Ahora, es necesario calcular el parámetro que se forma de la expresión:

$$\beta = q2^{n-i} \quad (3)$$

con base en lo anterior, se encontraron los siguientes parámetros para el mapa 1 y el mapa 2 respectivamente:

- $\beta_1 =$ .
- $\beta_2 =$ .

Se utilizó el siguiente código para la ejecución de las pruebas NIST:

- **./assess 2560000**
- User Prescribed Input File: **dosRenyisIntercambio2idifj.dat**
- Enter 0 if you DO NOT want to apply all of the statistical tests to each sequence and 1 if you DO. Enter choice: **1**
- How many bitstreams? **1**
- Input File Format: [0] ASCII - A sequence of ASCII 0's and 1's [1] Binary - Each byte in data file contains 8 bits of data  
Select input mode: **1**

### III-B. Resultados.

No se obtuvieron buenos resultados: no se aprobó ninguna prueba NIST.

## IV. CONCLUSIONES.

## V. ANEXOS.