Algoritmo LFSR versión de Fibonacci por Mario Jesús Carranza Castillo

INSTRUCCIONES

Primeramente, para poder ejecutar este ejercicio debe usar algún simulador de procesador RISC-V como Ripes. Este es posible encontrarlo en https://github.com/mortbopet/Ripes/releases

Para poder ejecutar el programa debe seguir los siguientes pasos:

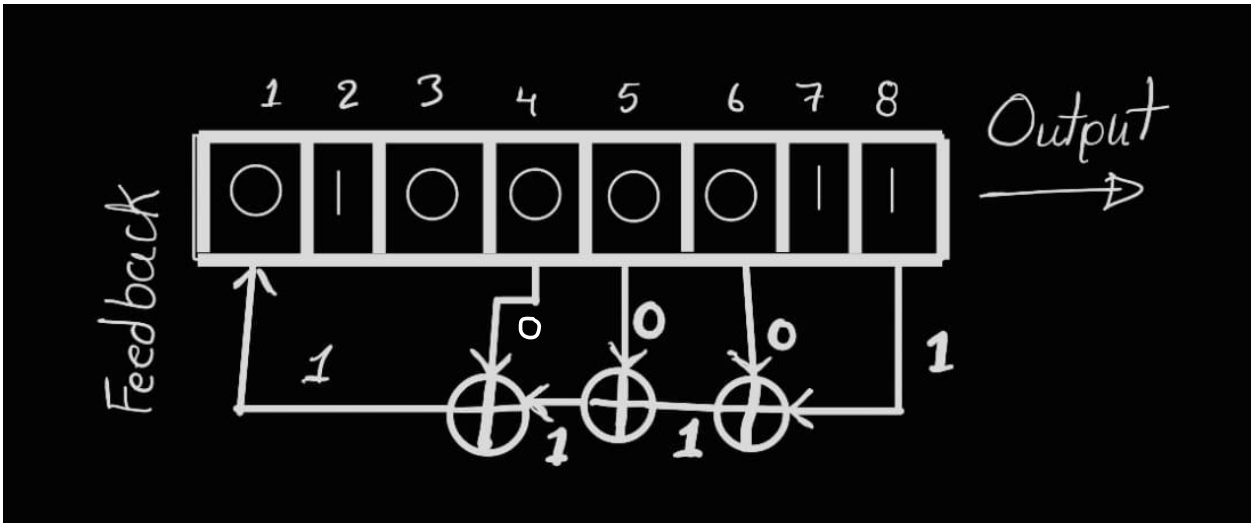
1. Abrir el simulador Ripes.
2. Cargar el archivo llamado ejercicio.s en File > Load Program.
3. En la opción del editor es posible ver el código debidamente comentado con cada uno de los pasos realizados para comprender el algoritmo LFSR en este caso con la versión de fibonacci. El valor semilla utilizado es el código binario correspondiente a la letra mayúscula C (Pimera letra de mi segundo apellido) cuyo código ASCII es 67, en hexadecimal es 0x43 y en código binario es el 01000011.
   Si se quiere cambiar el valor semilla, hágalo en dentro del código en la sección "main:" específicamente la línea 8 cambiando el valor 0x43 en hexadecimal. Si desea cambiar el número de iteraciones del algoritmo, debe hacerlo en la línea 9 del código cambiando el número 100 (en decimal) por el número que desee.
4. Por último, presione el botón para correr el programa en la parte superior de la pantalla.
5. Una vez ejecutado el programa, es posible ver los 100 resultados generados en la sección "Memory" los cuales se ubican desde la posición en memoria 0x100 en adelante.
6. Si lo desea, en la posición de memoria 0xf4 puede ver la secuencia de bits que fueron desplazados en cada iteración del algoritmo.

FUNCIONAMIENTO DEL ALGORITMO

Este generador tiene múltiples aplicaciones: criptografía, videojuegos, simulación y otros.

1. Se inicia con un valor semilla (inicial).
2. Luego pasa por una serie de compuertas XOR, que toman los bits de las posiciones del polinomio LFSR (para este caso se utiliza el polinomio LFSR: $x^8 + x^6 + x^5 + x^4 + 1$).
3. Se hace rotación a la derecha del resultado, el bit resultado del polinomio se coloca en el MSB del registro, se descarta el bit LSB.
4. Se actualizan los valores del registro y se realiza de nuevo el paso 1.

A continuación, se muestra el funcionamiento del algoritmo de manera gráfica utilizando la semilla antes mencionada.



El código generado implementa este algoritmo utilizando el set de instrucciones RISC-V.