LFSR

De Wikipedia, la enciclopedia libre

LFSR significa **linear feedback shift register**, que se traduce como: registro de desplazamiento con retroalimentación lineal. Es un registro de desplazamiento en el cual la entrada es un bit proveniente de aplicar una función de transformación lineal a un estado anterior.

El valor inicial se denomina semilla y, como la forma de operar el registro es determinista, la secuencia de valores producidos está completamente determinada por el estado actual o el estado anterior. La secuencia tiene un periodo de repetición, es decir que la secuencia vuelve a generarse y se repite indefinidamente. Cuando el periodo de repetición es máximo, ese LFSR tiene interés criptográfico.

Índice

Cómo trabaja LFSR

Veamos un ejemplo, tenemos la secuencia [16,14,13,11].

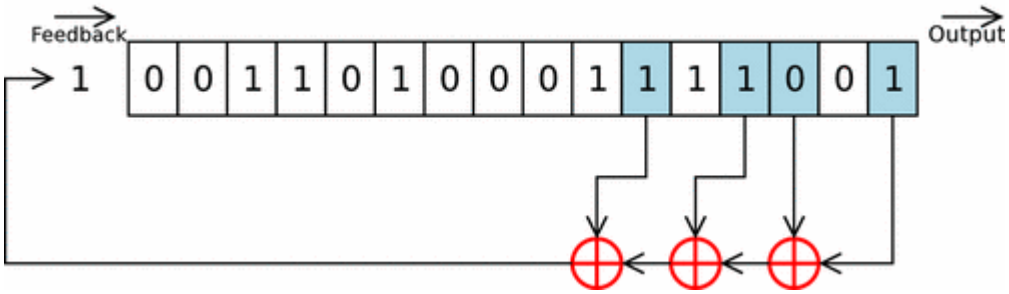
La secuencia tap de un LFSR se puede representar como un polinomio mod 2. Esto significa que los coeficientes del polinomio deben ser 1's o 0's. Esto se llama polinomio de realimentación o característica polinomial.

Por ejemplo, si los taps están en las posiciones de los bits: 16, 14, 13 y 11 ,el polinomio LFSR resultante es:

$$x^{11} + x^{13} + x^{14} + x^{16} + 1$$

Las salidas que influyen en la entrada, se denominan *taps*. Son las que aparecen en el polinomio. Y se indican en azul en el esquema inferior.

- Si el polinomio es primitivo, sí y solo sí, el LFSR es máximo, o lo que es lo mismo, tiene periodo máximo.
- El LFSR sólo será máximo si el número de taps es par.
- Los valores de tap en un LFSR máximo son coprimos.
- Puede haber más de una secuencia tap que haga máximo al LFSR para esa longitud determinada.
- Una vez encontrada una secuencia tap máxima, automáticamente sigue otra. Si la secuencia tap, en un LFSR n-bit, es [n,A,B,C], entonces la secuencia *mirror* correspondiente es [n,n-A,n-B,n-C]. Por ejemplo, la secuencia tap [32,3,2,1], tiene su homólogo [32,29,30,31]. Ambos dan como resultado periodo máximo.



Propiedades del flujo de salida

Un LFSR se puede caracterizar de forma polinómica según sean sus conexiones y los valores de los registros.

Se define el polinomio de Estado como:

$$S(D) = S_0 + S_1 D + S_2 D^2 + \ldots + S_n D^n$$

El polinomio de estado muestra el valor de los registros.

De la misma forma se define el polinomio de Conexiones como:

$$C(D) = C_0 + C_1 D + C_2 D^2 + \ldots + C_n D^n + C_{n+1} D^{n+1}$$

Donde cada coeficiente C_i vale 0 o 1 dependiendo de si hay conexión o no. Hay que notar que el polinomio de conexiones es siempre un grado mayor que el de estado.

De esta manera un LFSR con *n* registros de desplazamiento tendrá como mínimo 2 conexiones la de C_0 y la de C_{n+1}. La conexión de C_0 es necesaria porque sin ella el primer registro siempre valdría cero y por tanto no influiría en el comportamiento del LFSR. La conexión C_{n+1} es necesaria porque asegura la retroalimentación del LFSR. Si este coeficiente valiera 0 (o lo que es lo mismo, no hubiera esta conexión), el LFSR ya no sería de grado *n+1*.

De la misma forma De esta manera para pasar de un estado al siguiente los registros se desplazan. Este desplazamiento se puede expresar en forma polinómica como una multiplicación por D. El polinomio resultante tiene grado *n+1* al igual que el polinomio de conexiones. Esto es un problema ya que el polinomio de estado tiene que ser de grado *n*. Esto se soluciona haciendo que el polinomio resultante sea módulo de *C(D)*.

Si $S^{(i)}(D)$ es el polinomio de Estado en el estado *i-ésimo*, en forma polinómica el desplazamiento del polinomio de Estado se expresa así:

$$S^{(i+1)}(D) = S^{(i)}(D) \cdot D = S_0 D + S_1 D^2 + S_2 D^3 + \ldots + S_n D^{n+1}$$

Como el grado tiene que ser menor que *n+1* se hace el módulo de *C(D)*:

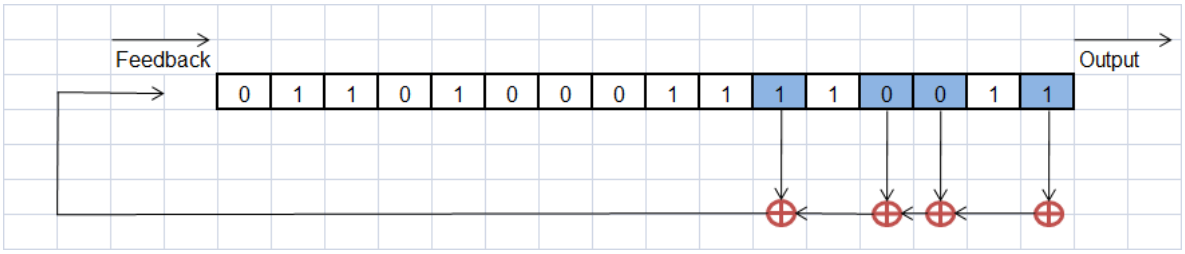
$$S^{(i+1)}(D) = S^{(i)}(D) \cdot D \mod C(D)$$

Con lo que resulta un polinomio de grado *n* como máximo.

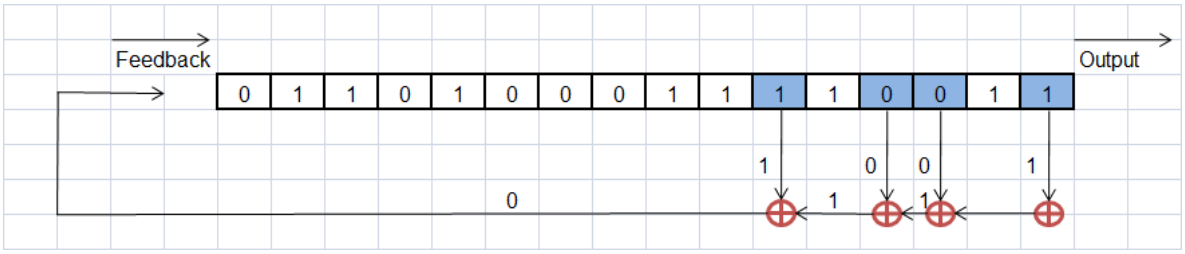
Usos criptográficos

Ejemplo de Wikipedia (Corregido)

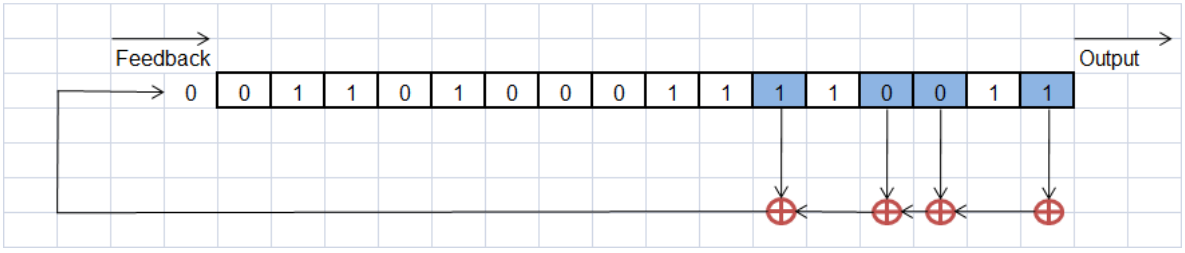
Paso 1:



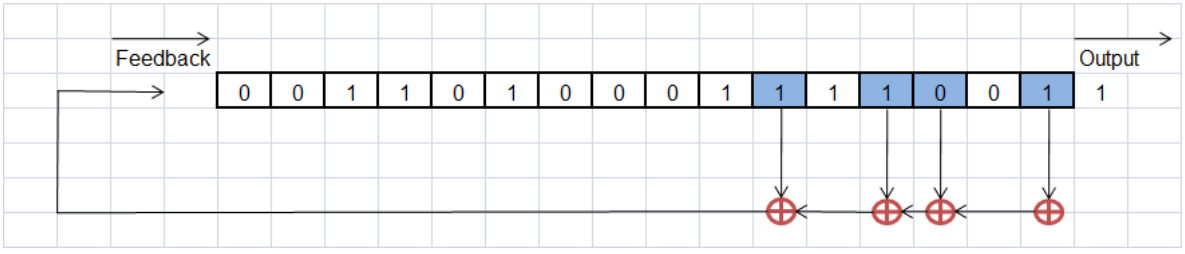
Paso 2:



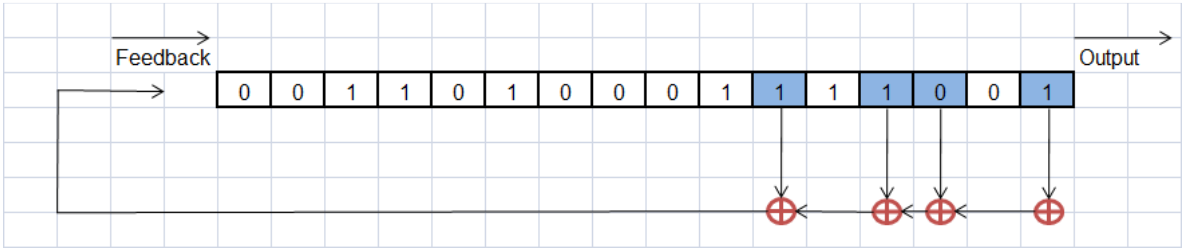
Paso 3:



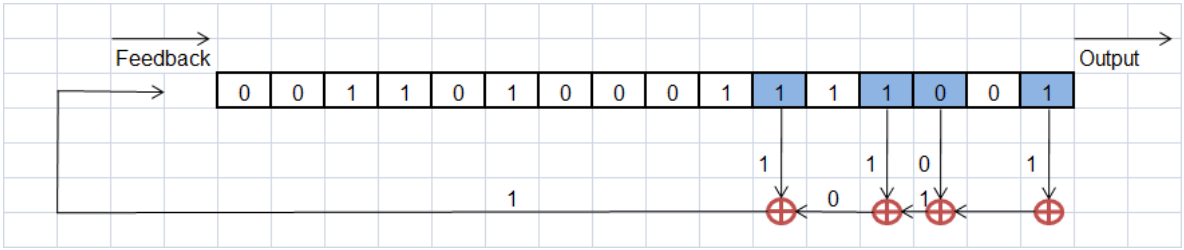
Paso 4:



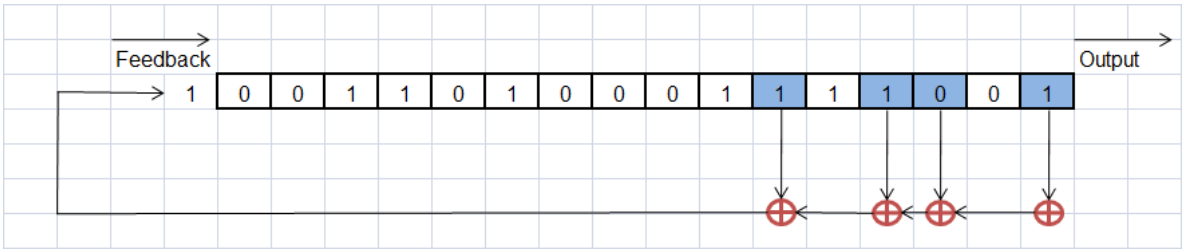
Paso 5:



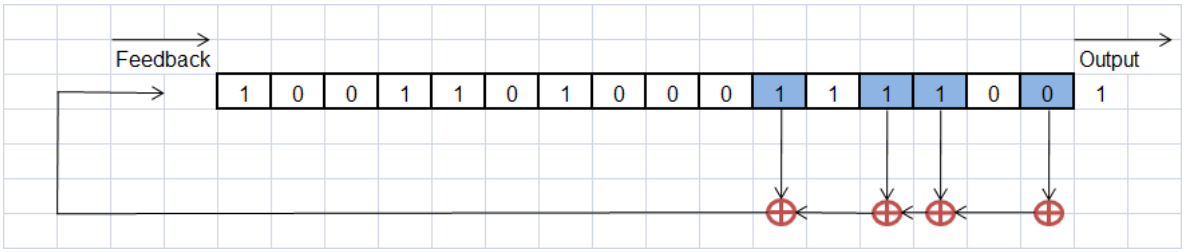
Paso 6:



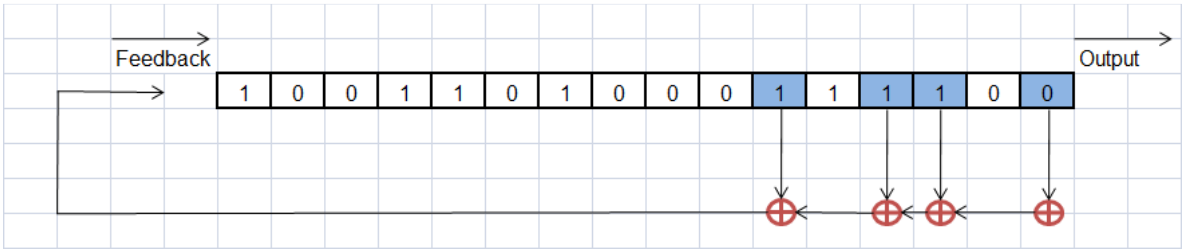
Paso 7:



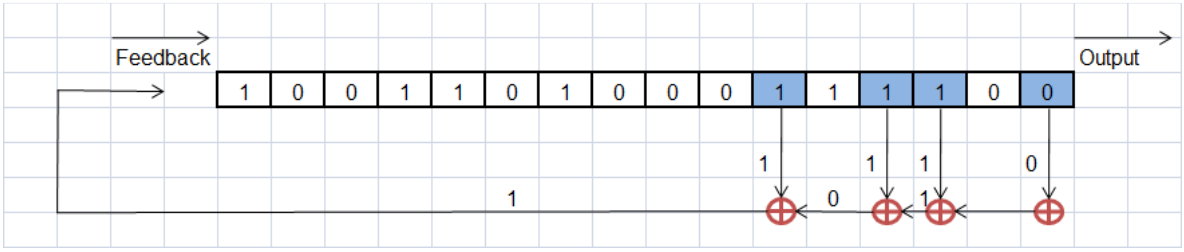
Paso 8:



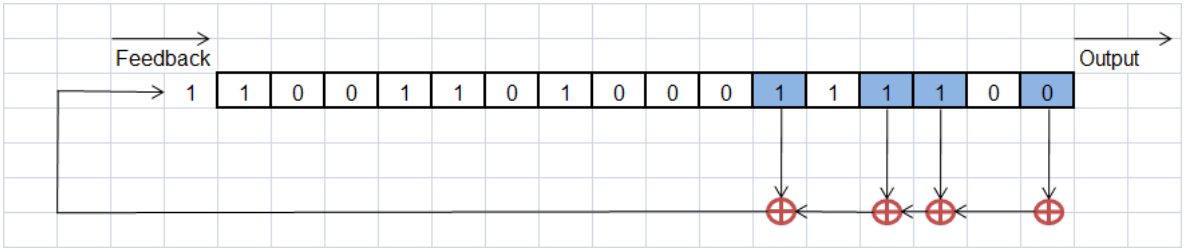
Paso 9:



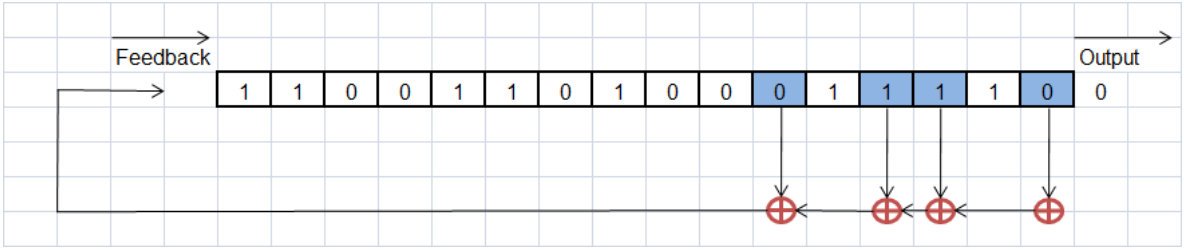
Paso 10:



Paso 11:



Paso 12:



Paso 13: