AMPLIACIÓN DE MATEMÁTICAS

CIFRADO EN FLUJO.

Un mensaje digital no es más que una colección de 0's y 1's ordenados. Por ejemplo:

$$0010110010.$$

Una forma de **cifrar** (de enmascarar) el menaje es la siguiente:

- tomamos una sucesión **periódica** de 0's y 1's, por ejemplo

  $$010010010010....etc$$

  (ésta tiene un periodo tres);
- para **cifrar** nuestro mensaje le sumamos nuestra sucesión periódica (término a término en $\mathbb{Z}_2$); por ejemplo

  $$\begin{array}{r} 0010110010 \\ +\underline{0100100100} \\ 0110010110, \end{array}$$

  (no confundir con la suma de números en base dos); esta 'suma' es el mensaje a enviar;
- para **descifrar** el mensaje enviado se vuelve a sumar nuestra sucesión periódica; por ejemplo

  $$\begin{array}{r} 0110010110 \\ +\underline{0100100100} \\ 0010110010, \end{array}$$

  llegando al mensaje original.

Este es un método de cifrado **simétrico,** en el sentido de que necesitamos la misma **clave** tanto para cifrar como para descifrar.

Para este sistema de encriptación necesitamos una '**máquina**' que genere 0's y 1's. Para ello vamos a considerar una función:

$$\begin{array}{rccc} f & : & \{0,1\}^n & \to & \{0,1\} \\ & & (s_0, s_1, ..., s_{n-1}) & \to & f((s_0, s_1, ..., s_{n-1})) = s_n. \end{array}$$

y construimos una 'máquina' F.S.H (feedback shift registers)

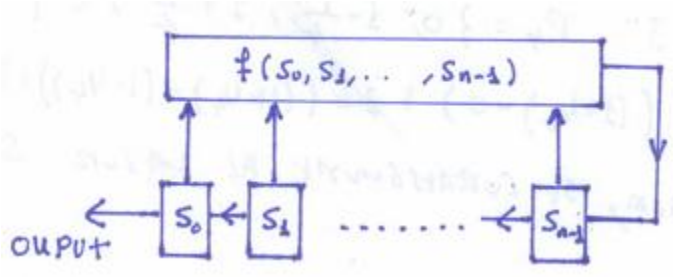

FIGURA 1. Máquina F.S.H.

Esta máquina F.S.H., de **longitud n**, contine n celdas de memoria. Al principio, juntas forman un **estado inicial**

$$(s_0, s_1, ..., s_{n-1}).$$

La función f toma el estado inicial y nos devuelve un valor s_n, con el cuál el estado inicial se transforma en

$$(s_1, s_2, ..., s_n)$$

y la máquina nos da como salida (**ouput**) el valor s_0. Al repetirse el proceso la máquina tiene como salida una sucesión de ceros y unos:

$$s_0, s_1, ..., s_{n-1}, s_n, s_{n+1}.....$$

Observación 1. **a:** *La función f más sencilla que podemos tomar es una función **lineal**, es decir algo de la forma*

$$f((s_0, s_1, ..., s_{n-1})) = c_0 s_0 + c_1 s_1 + ... + c_{n-1} s_{n-1} = s_n,$$

*con $c_0, ...c_{n-1} \in \mathbb{Z}_2$; siempre se toma $c_0 = 1$ y donde vemos que solo intervienen sumas y productos. Con una función de este tipo es muy fácil construir **físicamente** una máquina L.F.S.H. (linear feedback shift registers)*

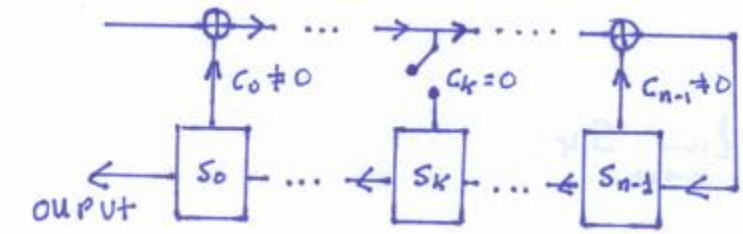

FIGURA 2. Máquina L.F.S.H.

Se puede probar *que cualquier función f en la construccción de una máquina F.S.H. se puede sustituir por otra función g lineal.*

b: *Toda máquina finita genera un proceso periódico. Por ello, solo podemos esperar de nuestra máquina L.F.S.H que produzca una sucesión periódica de ceros y unos*

$$(s_0, s_1, ...s_{n-1}.....) = (s_j)_{j=0}^{\infty}$$

*de modo que $s_{j+k} = s_j$ para dodo $j \in \mathbb{N}$ y para cierto $k \in \mathbb{N}$ (**el periodo**). En nuestro ejemplo de arriba el periodo $k = 3$.*

c: *Para que la sucesión periódica de ceros y unos $(s_j)_{j=0}^{\infty}$ tenga buenas **propiedades criptográficas** se necesita que:*

- *el **periodo** k sea **grande** partiendo de un n asumible físicamente (el estado inicial consta de n registros prefijados).*
- *Que la sucesión $(s_j)_{j=0}^{\infty}$ parezca casi **aleatoria** (es decir que se parezca a un **ruido** mezclado por azar en el mensaje y no algo generado por una máquina).*
- *Que sea fácil de obtener y manejar.*

El problema que tenemos entre manos es elegir "adecuadamente" las coeficientes de la función

$$f(s_0, s_1, ..., s_{n-1}) = \sum_{i=0}^{n-1} c_i s_i = s_n$$

o en forma matricial

$$(*) \qquad \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & & & \vdots \\ & & & & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ c_0 & c_1 & \cdots & & c_{n-2} & c_{n-1} \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ \\ s_{n-2} \\ s_{n-1} \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ \\ s_{n-1} \\ s_n \end{pmatrix} \equiv \quad \text{mód} \quad 2.$$

de modo que la sucesión periódica de salida $(s_j)_{j=0}^{\infty}$ tenga las mejores propiedades criptográficas señaladas en la Observación anterior. En primer lugar veamos cuánto de grande es la sucesión de salida.

Lema 1. *Un L.F.S.H. de longitud n genera a lo más una sucesión de periodo $2^n - 1$.*

Demostración: Partimos siempre de un estado inicial

$$(s_0, s_1, ..., s_{n-1}) \neq (0, 0, ..., 0),$$

el estado inicial nulo solo genera la sucesión nula. Como al menos $c_0 \neq 0$, partiendo del estado inicial, generamos los estados

$$(s_1, s_2, ..., s_n), (s_2, s_3, ..., s_{n+1}), ...\text{etc.}$$

Como s_j solo puede tomar dos valores (0 o 1), el núnero de estados distintos solo pueden ser a lo más $2^n - 1$ (el estado nulo $(0, 0, ..., 0)$ nunca se produce por la transformación $(*)$, repasa el Algebra Lineal de Primer curso). Y por tanto en el estado 2^n-ésimo hay seguro una repetición $\square$

Observación 2. *$2^n - 1$ es el orden del grupo cíclico multiplicativo $((\mathbb{Z}_2[x]/p(x))^*, \times)$ donde $p \in \mathbb{Z}_2[x]$ es un polinomio irreducible de grado n. ¿Estamos ante una simple coincidencia? La respuesta es que **no**.*

Definición 1. *Dada una función líneal*

$$\begin{array}{ccccc} f & : & \mathbb{Z}_2^n & \to & \mathbb{Z}_2 \\ & & (s_0, s_1, ..., s_{n-1}) & \to & f((s_0, s_1, ..., s_{n-1})) = c_0 s_0 + c_1 s_1 + ... + c_{n-1} s_{n-1} = s_n, \end{array}$$

*con $c_0 \neq 0$, se llama **polinomio característico** de la función lineal f al polinomio $p \in \mathbb{Z}_2[x]$ definido por*

$$p(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1} + x^n.$$

Si p es irreducible, como es de grado n, el cuerpo que genera $\mathbb{Z}_2[x]/p$ tiene cardinal 2^n. El grupo multiplicativo $((\mathbb{Z}_2[x]/p(x))^*, \times)$ tiene orden $2^n - 1$ y es cíclico. Así podemos encontrar (¡aunque esto no es nada sencillo!) un **elemento primitivo**

$$\alpha \in ((\mathbb{Z}_2[x]/p(x))^*, \times)$$

que tiene la propiedad de ser un generador del grupo. Asociado a él podemos encontrar un polinomio mínimo $q(x)$ con respecto a $\mathbb{Z}_2[x]$, es decir un polinomio mónico irreducible de grado n de modo que $\overline{q}(\alpha) = 0$. Este polinomio sabemos que existe y lo llamamos **polinomio primitivo** asociado a α. Sea

$$q(x) = c_0' + c_1' x + ... + c_{n-1}' x^{n-1} + x^n$$

donde $c_0' \neq 0$ (en otro caso no sería irreducible).

Observación 3. ***Se puede probar*** *que si el polinomio $p \in \mathbb{Z}_2[x]$ asociado a una función lineal f es* ***primitivo,*** *entonces la sucesión de ceros y unos $(s_j)_{j=0}^{\infty}$ que genera f tiene período máximo, es decir $2^n - 1$. (Lo cuál solo ocurre si p es primitivo).*

Además, ***se puede ver*** *que la sucesión tiene buenas propiedades criptográficas, en el sentido de que la sucesión $(s_j)_{j=0}^{\infty}$ es "casi" aleatoría (concepto que no tenemos tiempo de explicar en esta asignatura).*

Por lo anterior, es importante conocer los polinomios irreducibles y entre ellos los primitivos sobre $\mathbb{Z}_2[x]$ de cualquier grado. Este estudio ya queda fuera de nuestras posibilidades.

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain
E-mail address: Cesar_Ruiz@mat.ucm.es