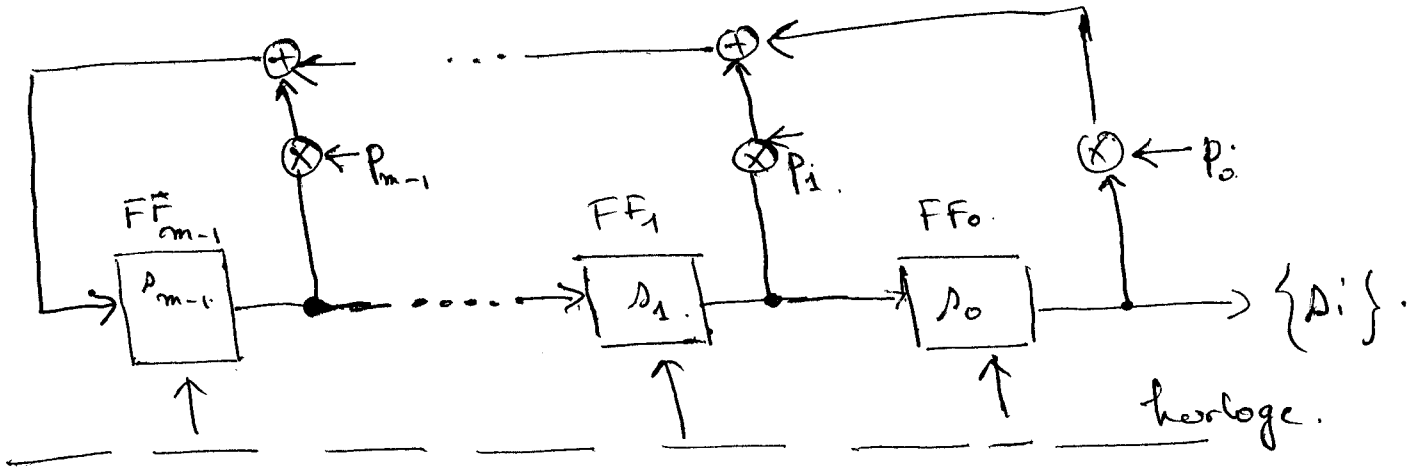
(5). S-cryptage basé sur les Registres à décalage.

- La s-clé $s_1, s_2, \ldots$ est engendré par un LSFR; facile à implémenter hardware, servent en GSM parce. On peut les rendre résistants aux attaques. On verra les bases ici.

- (5.1) LSFR. La forme d'un LSFR de degré m est:



avec les $p_i \in \{0, 1\}$; $p_i = 1$. (resp 0) si feed-back actif (resp. non actif).

FF_i : flip-flop. contenant la valeur initial s_i $(i = 0, \ldots, m-1)$

ainsi $s_m = s_{m-1} p_{m-1} + \cdots + s_0 p_0 \mod 2$.

$s_{m+1} = s_m p_{m-1} + \cdots + s_1 p_0$, etc.

En général la partie s_{i+m} est:

$$s_{i+m} = \sum_{j=0}^{m-1} p_j s_{i+j}$$

Théorème. La période maximale d'un LSFR est $2^m - 1$.

Preuve. Compter le nombre d'états du LSFR. ⊕