Générateurs de nombres aléatoires
Cours 2 - Registres à décalage à rétroaction linéaire (LFSR)

A. Ridard

École d'ingénieurs ensibs
Université Bretagne Sud

A propos de ce document

- Pour naviguer dans le document, vous pouvez utiliser :
  - le menu (en haut à gauche)
  - les différents liens
- Pour signaler une erreur, vous pouvez envoyer un message à l'adresse suivante : anthony.ridard@univ-ubs.fr

Plan du cours

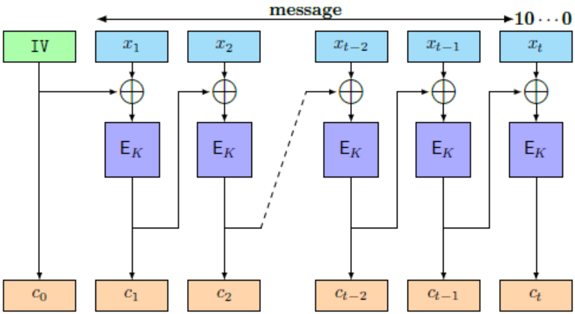
1. A quoi sert l'aléa cryptographique ?
2. Registres à décalage à rétroaction linéaire (LFSR)
3. Augmenter la complexité d'un LFSR

Rappelons[1] les différentes primitives cryptographiques et leur objectif de sécurité :

<table>
<tr><th colspan="2">Service</th><th>Cryptographie symétrique</th><th>Cryptographie asymétrique</th></tr>
<tr><td colspan="2" rowspan="2">Confidentialité</td><td rowspan="2">Chiffrement conventionnel par bloc (A.1.1.1)
ou par flot (A.1.1.2)</td><td>Chiffrement à clé publique (A.2.1)</td></tr>
<tr><td>Échange de clé (A.2.3)</td></tr>
<tr><td colspan="2">Intégrité</td><td rowspan="2">Code d'authentification de message (A.1.3)</td><td rowspan="4">Signature numérique (A.2.2)</td></tr>
<tr><td rowspan="2">Authentification</td><td>de données</td></tr>
<tr><td>d'entités</td><td>Défi-réponse (A.1.4)</td></tr>
<tr><td colspan="2">Non-répudiation</td><td>Aucune primitive</td></tr>
</table>

1. Ce tableau est extrait du Référentiel Général de sécurité - Annexe B1 - édité par l'ANSSI

Pour traiter des messages de taille quelconque et assurer la confidentialité globale de ces messages, et pas uniquement une confidentialité « par bloc », il convient de définir un **mode opératoire** précisant comment convertir le message en une suite de blocs ainsi que le mode de chiffrement de ces blocs afin d'obtenir finalement le message chiffré [2]. Enfin, pour rompre le caractère déterministe du chiffrement, il est nécessaire de « randomiser » le processus, c'est-à-dire d'introduire une valeur aléatoire.



2. Notons que la définition d'un tel mode opératoire n'a nul besoin de tenir compte des détails de l'algorithme de chiffrement par bloc employé, seul la taille des blocs est réellement nécessaire

Un GPA (binaire) permet de chiffrer un message long m avec une clé courte :

- La clé secrète est la graine du GPA
- Pour chiffrer m de longueur l, on utilise la suite chiffrante $s = (s_0, \dots, s_{l-1})$:

$$c = m \oplus s$$

- Pour déchiffrer le message reçu, le destinataire doit **reproduire** la même suite chiffrante à partir de la clé secrète, puis utiliser le XOR :

$$c \oplus s = (m \oplus s) \oplus s = m \oplus (s \oplus s) = m \oplus 0 = m$$

Par rapport au masque jetable de Vernam, ce chiffrement évite la transmission préalable d'une quantité d'aléa aussi importante que le message à chiffrer !

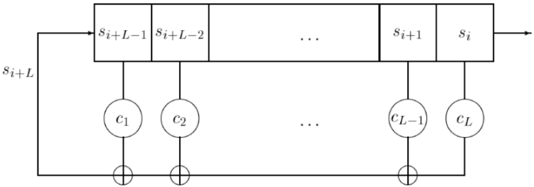
Un registre à décalage à rétroaction linéaire [3] (binaire) de longueur L est composé :

- d'un registre à décalage contenant une suite de L bits $(s_i, \ldots, s_{i+L-1})$
- et d'une fonction de rétroaction linéaire

A chaque top d'horloge, le bit de poids faible s_i constitue la sortie du registre, et les autres sont décalés vers la droite ; le nouveau bit s_{i+L} placé dans la cellule de poids fort du registre est donné par une fonction linéaire :

$$s_{i+L} = c_1 s_{i+L-1} \oplus c_2 s_{i+L-2} \oplus \cdots \oplus c_{L-1} s_{i+1} \oplus c_L s_i$$

où les coefficients c_i sont binaires.



Pour visualiser le fonctionnement, une animation est disponible ici

3. On l'appelle aussi par son acronyme anglais : LFSR (Linear Feedback Shift Register)

En notant R_n le n-ième registre et $A = \begin{pmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ c_L & c_{L-1} & \dots & c_2 & c_1 \end{pmatrix}$, on a :

- $R_{n+1} = AR_n$
- $R_n = A^n R_0$
- $\det(A) = c_L$

On peut alors montrer :

- La suite $s = (s_n)_{n\in\mathbb{N}}$ est ultimement périodique de période $T \leq 2^L - 1$
- Si $c_L = 1$, elle est même périodique

Son polynôme de rétroaction est le polynôme f de $\mathbb{F}_2[X]$ défini par :

$$f(X) = 1 + c_1 X + c_2 X^2 + \cdots + c_L X^L$$

Sa série formelle de $\mathbb{F}_2[[X]]$ est définie par :

$$s(X) = \sum_{n \in \mathbb{N}} s_n X^n$$

Son polynôme de rétroaction minimal est l'unique polyn. unitaire f_0 de $\mathbb{F}_2[X]$ tel que :

$$s(X) = \frac{g_0}{f_0}$$

avec $g_0 \in \mathbb{F}_2[X]$ vérifiant $\deg(g_0) < \deg(f_0)$ et $pgcd(g_0, f_0) = 1$

On peut alors montrer :

- Sa complexité linéaire[4] est le degré de f_0
- Si f_0 est primitif[5], alors la période est maximale

4. Longueur du plus petit LFSR produisant la suite $s = (s_n)_{n \in \mathbb{N}}$
5. Une de ses racines engendre le groupe multiplicatif $(\mathbb{F}_{2^L})^*$

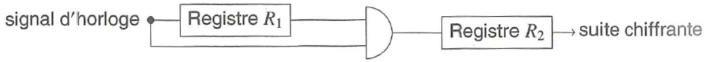
Même si la période est maximale, la complexité linéaire de la suite produite est trop faible pour permettre une utilisation cryptographique. A partir de l'observation de suffisamment [6] de bits consécutifs, on peut déterminer la complexité linéaire l et reconstruire le polynôme de rétroaction minimal (TP) avec un coût [7] en $O(l^4)$.

6. Le double de la complexité linéaire de la suite
7. L'algorithme de Berlkamp-Massey permet même de résoudre ce problème avec un coût en $O(l^2)$

Les registres à décalage irrégulier ont une horloge interne contrôlée par un autre LFSR.

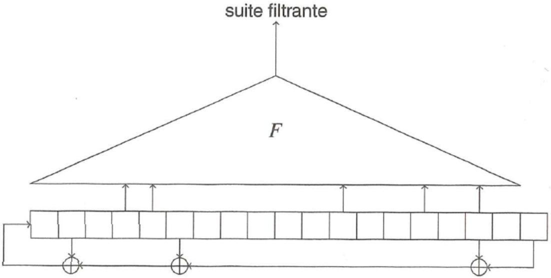
Exemples :

- Le générateur à signal d'arrêt (TP)



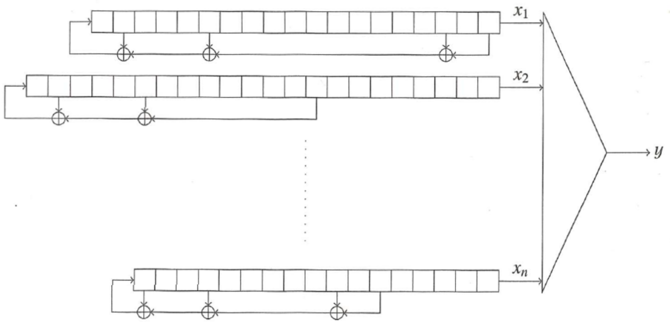
- Le générateur par rétrécissement (ou sa variante par auto-rétrécissement)

Les registres à rétroaction linéaire filtrés appliquent une fonction non linéaire à certains bits de l'état interne d'un LFSR.



Exemple : Générateur Toyocrypt

Les registres à rétroaction linéaire combinés appliquent une fonction non linéaire aux bits de sortie de plusieurs LFSR.



Exemple : Générateur de Geffe (TP)

Ce cours s'appuie principalement sur :

- le Référentiel Général de Sécurité - Annexe B1
- le livre "Exercices et problèmes de cryptographie" de Damien Vergnaud