Master CSI 2 2019-2020

Cryptanalyse — 4TCY902U

Responsable : G. Castagnos

TP 5 — LFSR

1 LFSR

1. Écrire une fonction qui simule une étape d'un LFSR : elle doit prendre en entrée l'état au temps t et un polynôme de rétroaction et ressortir l'état au temps $t+1$ et le bit de sortie (on supposera que le degré du polynôme est égal à la longueur de l'état).

2. En déduire une fonction prenant en paramètres un état initial $S^{(0)}$, un polynôme de rétroaction f et un entier N et retournant les N premiers bits de sortie du LFSR de rétroaction f et initialisé par $S^{(0)}$. Pour tester votre fonction, le LFSR de longueur 5 et de polynôme de rétroaction $f(X) = X^5 \oplus X^4 \oplus 1$, initialisé par 00101 retourne la suite 00101011111000010011 ...

2 On s'intéresse maintenant aux cycles des registres d'un LFSR.

1. Écrire une fonction prenant en paramètre l'état initial $S^{(0)}$ du LFSR et le polynôme de rétroaction (de même degré que la longueur des registres) et retournant le cycle des registres obtenus, c'est à dire la liste des différents états obtenus dans une période : $S^{(0)}, S^{(1)}, \dots, S^{(T)}$ avec $S^{(0)}, S^{(1)}, \dots, S^{(T-1)}$ tous distincts et $S^{(0)} = S^{(T)}$.

2. Tester avec $f(X) = X^5 \oplus X^4 \oplus 1$ et les états initiaux 00101, 01000 et 10100. Que remarquez vous ?

3. Écrire une fonction prenant en paramètre le polynôme de rétroaction et retournant tous les cycles de registres possibles (en faisant varier l'état initial).

4. Combien de cycles produit le LFSR de longueur 5 de polynôme de rétroaction f ? Même question avec les LFSR de longueur 4 de polynômes de rétroaction $1 \oplus X^2 \oplus X^4$, $1 \oplus X \oplus X^2 \oplus X^3 \oplus X^4$ et $1 \oplus X \oplus X^4$. Quelles sont les propriétés de ces divers polynômes ?

5. Écrire une fonction qui prend en paramètre f et un état initial et qui renvoie le polynôme g telle que $Z(X) = g(X)/f(X)$ soit la série formelle du LFSR engendré par f et initialisé par l'état initial. Tester dans les différents cas de la question précédente si f est le polynôme minimal.

3 On note $(z_i)_{i \geq 0}$ la suite produite par un LFSR de polynôme de rétroaction $X^7 \oplus X^6 \oplus 1$. On suppose que cette suite vérifie $z_{2i} = z_i$ pour tout $i \geq 0$. Quel est l'état initial $(z_0, z_1, \dots, z_6)$ du LFSR ?

4 Trace et LFSR

1. soit $\mathbf{F} = \mathbf{F}_{2^\ell}$. On pose, pour tout $\alpha \in \mathbf{F}$,

$$\mathrm{trace}(\alpha) = \alpha \oplus \alpha^2 \oplus \alpha^4 \oplus \cdots \oplus \alpha^{2^{\ell-1}}.$$

   (a) Montrez que $\mathrm{trace}(\alpha) \in \mathbf{F}_2$.

   (b) Montrez que $\mathrm{trace}(\alpha) \oplus \mathrm{trace}(\beta) = \mathrm{trace}(\alpha \oplus \beta)$ pour tout $\alpha, \beta \in \mathbf{F}$.

   (c) Soit $\alpha \in \mathbf{F}$. Montrez que, si $\mathrm{trace}(\alpha u) = 0$ pour tout $u \in \mathbf{F}$, alors $\alpha = 0$.

2. Soit $f(X) = 1 \oplus c_1 X \oplus c_2 X^2 \oplus \cdots \oplus c_\ell X^\ell$ un polynôme de $\mathbf{F}_2[X]$ de degré ℓ que l'on suppose irréductible. On fixe une racine α de f dans $\mathbf{F}$ et on pose $\mathbf{F} = \mathbf{F}_2[\alpha]$.

   (a) On note $\gamma = \alpha^{-1}$. Montrer que la suite des $(\gamma^j)_{j \geqslant 0}$ est engendrée par un LFSR de polynôme de rétroaction f dans le corps $\mathbf{F}$. En déduire que pour tout $\beta \in \mathbf{F}$, la suite binaire définie par $z_j = \mathrm{trace}(\beta\gamma^j)$ pour $j \geqslant 0$ est également engendrée par un LFSR de polynôme de rétroaction f.

   (b) Combien de suites distinctes sont engendrées par f ? En déduire que toute suite engendrée par f est de la forme précédente.

   (c) Pour tout entier t, on note $z^{(t)}$ la suite définie par

$$\left(z^{(t)}\right)_j = z_{tj}, \forall\, j \geq 0.$$

   On dit que cette suite est une $t-$décimation de la suite z. Montrez que la suite $z^{(t)}$ est engendrée par le polynôme minimal de α^t sur $\mathbf{F}_2$.

   (d) Exemple : $f(X) = 1 \oplus X^3 \oplus X^4$. On sait que f est irréductible sur $\mathbf{F}_2$ et que ses racines engendrent $\mathbf{F}_{16}^*$. Soit z une suite non nulle engendrée par f. Quels sont les polynômes minimaux des suites $z^{(2)}$, $z^{(3)}$, $z^{(5)}$? Quelles sont leur période ?

5 On a partiellement intercepté une suite binaire dont on sait qu'elle est produite par un LFSR de longueur 5 :

$$1, 0, *, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, *, 0, 0, *, 1, 0, *, 1$$

Peut on retrouver les bits manquants et le polynôme de rétroaction ?