Cryptanalyse — M1MA9W06

Responsable : G. Castagnos

Devoir surveillé — 17 novembre 2015

Durée 1h30
accès aux fonctions programmées en TP, aux énoncés des TP et à la fiche d'initiation à Sage autorisés, autres documents non autorisés
Les deux exercices sont indépendants, cependant il est nécessaire d'avoir fait la question (c) de l'exercice 1 pour pouvoir faire les deux dernières questions de l'exercice 2.

1 Dans cet exercice, $z = (z_t)_{t\geqslant 0}$ désigne une suite binaire strictement périodique non constante produite par un LFSR de longueur ℓ et de polynôme de rétroaction $f(X) \in \mathbf{F}_2[X]$. On note $Z(X)$ la série génératrice définie par $Z(X) = \sum_{t\geqslant 0} z_t X^t$.

(a) Rappeler sans démonstration l'expression du polynôme $g(X) \in \mathbf{F}_2[X]$ tel que $Z[X] = g(X)/f(X)$.

(b) On suppose connaître les polynômes $g(X)$ et $f(X)$, montrer comment retrouver l'état initial du LFSR.

(c) Application, **avec Sage**, donner le code d'une fonction prenant en entrée g et f et ressortant cet état initial. Avec $g = X^{10} \oplus X^7 \oplus X^4 \oplus 1$ et $f = X^{15} \oplus X^5 \oplus X^4 \oplus X^2 \oplus 1$, quel est cet état initial ?

2 Une attaque par corrélation d'ordre 2

(a) On considère la fonction booléenne f en quatre variables, $f(x_1, x_2, x_3, x_4) = x_1 \oplus x_2x_4 \oplus x_2 \oplus x_3x_4$. Montrer que f est non corrélée à l'ordre 1, mais corrélée à l'ordre 2 (c'est à dire corrélée avec une somme de deux variables). La fonction f est elle équilibrée ? Pour répondre à cette question, on peut raisonner sans machine ou utiliser Sage (dans ce cas fournir le code utilisé).

(b) On considère les 4 LFSR suivants :

- LFSR1 de longueur 5 de polynôme de rétroaction $P_1(X) = X^5 \oplus X^2 \oplus 1$;
- LFSR2 de longueur 7 de polynôme de rétroaction $P_2(X) = X^7 \oplus X \oplus 1$;
- LFSR3 de longueur 9 de polynôme de rétroaction $P_3(X) = X^9 \oplus X^4 \oplus 1$;
- LFSR4 de longueur 11 de polynôme de rétroaction $P_4(X) = X^{11} \oplus X^2 \oplus 1$.

Avec Sage : Donner les 10 premiers bits de sortie du générateur combinant les sorties de ces quatre LFSR avec la fonction f, en utilisant pour initialisations des 4 LFSR les clefs $K_1 = [1,0,1,0,1]$, $K_2 = [1,0,1,0,1,0,1]$, $K_3 = [1,0,1,0,1,0,1,0,1]$ et $K_4 = [1,0,1,0,1,0,1,0,1,0,1]$. Expliquer la méthode, ne pas donner tout le code utilisé.

(c) Quelle est la complexité linéaire de la suite produite par ce générateur ? Bien justifier le résultat, en particulier, préciser les éventuelles commandes Sage utilisées.

(d) Soit z une suite de sortie de ce générateur, avec des initialisations inconnues. En s'inspirant de l'attaque par corrélation, expliquer comment trouver l'initialisation d'un LFSR de polynôme de rétroaction $P_1 \times P_2$ produisant une suite z' « proche » de z.

(e) Application **avec Sage** : Récupérer une telle suite z par la commande

```
load("http://www.math.u-bordeaux1.fr/~gcastagn/z.sage")
```

Donner cette initialisation ainsi que le polynôme g tel que $g(X)/(P_1(X)P_2(X)) = Z'(X)$ la série formelle associée à la suite z'.

(f) À l'aide d'une relation de Bézout entre P_1 et P_2, trouver **avec Sage**, un polynôme g_1 avec $deg\, g_1 < deg\, P_1$ et un polynôme g_2 avec $deg\, g_2 < deg\, P_2$ tels que $Z'(X) = g_1/P_1 + g_2/P_2$. Expliquer la méthode, et donner le code utilisé.

(g) En déduire **avec Sage** l'initialisation des LFSR1 et des LFSR2 ayant produit la suite z.

(h) Donner une méthode pour trouver l'initialisation des LFSR3 et des LFSR4 ayant produit la suite z et sa complexité. Programmer cette attaque avec Sage et donner ces initialisations.