Ahmed Saadi

Projet de Cryptographie symétrique (réponses aux questions)

1 . Générateur de type Geffe pour le chiffrement à flot :

1/ la réponse est incluse dans la page accompagnant le rapport au nom de : Geffe.c.

2/ le calcul théorique de la corrélation entre le générateur s¡ et la sortie LFSR S'explique par l'existence d'une éventuelle corrélation entre la sortie de la fonction de combinaison(f) et l'une de ses entrées tel qu'expliquer par la suite dans cet exemple de Probabilité de corrélation de la suite x1(t) à la suite s(t):

X0X1X2	F
000	1
100	0
010	0
110	0
001	1
101	1
011	1
111	0

{P(s(t) = x1(t)) = 1 } == ¾ , si x=0 il y'a 3 chance sur 4 que si soit égal 1

Donc P(s(t) = x0(t)) = 1/4

Cas général :

On joue sur Fi = 0 ou 1

P(si =1)\(x0 = 0) = (F0+F2+F4+F6)/4

P(si =1)\(x0 = 1) = (F1+F3+F5+F7)/4

P(si =1)\(x1 = 0) = (F0+F1+F4+F5)/4

P(si =1)\(x1 = 1) = (F2+F3+F7+F6)/4

P(si =1)\(x2 = 0) = (F0+F2+F3+F1)/4

P(si =1)\(x2 = 1) = (F7+F5+F4+F6)/4

3/ La première étape de l'attaque consiste à rechercher une corrélation entre la suite chiffrante et la sortie d'un des registres, on peut facilement se convaincre que la valeur du bit de la suite chiffrante est égale `a la valeur du bit de la sortie du LFSR L1 avec une probabilité de trois quart (¾).

La seconde étape consiste alors à attaquer ce registre-ci: on considère les unes après les autres les valeurs possibles pour son état interne, duquel on déduit la suite produite par ce registre que l'on compare avec la suite chiffrante du chiffrement entier. Si on observe la même corrélation que celle calculée en théorie, l'état interne est probablement le bon. Cette seconde étape correspond à réaliser une recherche exhaustive sur la valeur de l'état interne de L1, `. On peut ensuite finaliser l'attaque en faisant une recherche exhaustive sur les registres restants ou en recommençant cette attaque avec un autre registre aussi corrèle avec la suite chiffrante. Cette attaque se généralise `a des corrélations existantes entre la suite chiffrante et plusieurs registres : c'est ce qu'on appelle les corrélations d'ordre supérieur.

4/ pour trouver l'état initial de R1 on prendra 2 ^ (L1) essais.

En répétant l'opération pour les deux autres registres, l'état initial de chaque LFSR peut être déterminé en environ 2 ^L1 +2 ^L2 +2 ^L3 essais

Ce nombre est bien plus petit que le nombre de différentes clefs qui est environ 2 ^ L1+L2+L3

6/ Pour rendre l'attaque plus difficile il faut avoir moins de probabilité de corrélation entre f et les registres. , il faut avoir % de corrélation < à 50 %

Par exemple F = (1,1,1,0,1,0,0,0)

P(Fi=1) = P(Fi=0)= ½

Et la probabilité p de corrélation est inférieur à la moitié

2 .Un chiffrement par bloc faible

1/ On suppose que le chiffrement ne fait qu'un tour et on connaît :

X(L0) = 0100 0101 0000 0001 1001 1000 0010 0100

X(R0) = 0101 0001 0000 0010 0011 0011 0010 0001

De plus on a :

x(L)(r+1) = ((x(L) (r) ^ x(R)(r)) <<<7) ^ K0

X(L)(r+1) =((x(R)(r) ^x(L) (r+1) <<<7) ^K1

Donc :

X(L0) ^ X(R0) = 0001   0100 0000 0011 1010 1011 0000 0101

>>>7   = > 0000 0001 1101 0101 1000 0010 1000 1010

K0= 0000 0001 0000 0010 0000 0011 0000 0100

K0 ^ >>>7 = 0000 0000 1101 0111 1000 0001 1000 1110

(K0 ^ >>>7) ^ X(R0) = 0101 0001 1101 0101 1011 0010 1010 1111

(K0 ^ >>>7) ^ X(R0) >>> 7   = 1110 1010 1101 1001 0101 0111 1010 1000

K1= 0000 1001 1000 0111 0110 0101 0100 0011 0010

((K0 ^ >>>7) ^ X(R0) >>> 7) ^ K1 = 0111 0010 1010 1111 0000 0011 1001 1010

X(L1) = 0000 0000 1101 0111 1000 0001 1000 1110

Résultat final :

X(R1) = 0x72AF039A /// X(L1) 0xD7818E

2 / on suppose que le chiffrement ne fait qu'un tour et que l'on connait les textes (claire/chiffrés)

Ça nous donne :

K0=x(L)(r+1) ^((x(L)(r) ^x(R) (r)) <<<7)

K1 = x(L)(r+1) ^ ((x(R) (r) ^x(L)(r+1)) <<< 7)