Master CSI 2 2013-2014

Cryptanalyse — M1MA9W06
Responsable : G. Castagnos

TP 6 — Cryptanalyse linéaire de B32

B32 est un système de chiffrement par blocs proposé par Bart Preneel et Lars Knudsen pour s'initier aux mécanismes de la cryptanalyse différentielle et de la cryptanalyse linéaire.

C'est un système de type SPN qui opère sur des blocs de 32 bits. On se limitera à un schéma à deux tours utilisant trois clefs de 32 bits K_0, K_1, K_2.

Après l'étape initiale consistant à additionner K_0 au message clair, la fonction de tour opère de la façon suivante :

1. Substitution : Les 32 bits sont découpés en 8 blocs de 4 bits. Chaque bloc de 4 bits passe par une même S-box donnée par :

   $$S = [7,3,6,1,13,9,10,11,2,12,0,4,5,15,8,14].$$

   Il faut comprendre : l'image de i par S est $S[i]$, où $i \in [0..15]$ est identifiée avec son écriture binaire (bit de poids faible à droite !). Par exemple l'image de $[0,1,0,0]$ est donnée par $S[4] = 13$, c'est à dire $[1,1,0,1]$ [1].
2. Permutation : Le bloc subit un décalage circulaire de 2 vers la droite ;
3. On ajoute la clé de tour (K_1 au premier et K_2 au second).

1 Écrire une fonction de tour, une fonction de tour inverse, une fonction donnant le chiffrement complet à 2 tours avec 3 clés K_0, K_1, K_2 et la fonction de déchiffrement correspondante.

Il pourra être utile pour la clarté du code de traiter les blocs et les clefs comme des listes d'éléments de $\mathbf{F}_2$. De même, on pourra écrire des fonctions de conversions de séquences de 4 éléments de $\mathbf{F}_2$ vers les entiers de 0 à 15 pour l'appel aux boîtes S.

Pour tester la fonction : le chiffrement B32 de $(0,0,\ldots,0,0)$ avec les clefs $K_0 = (1,0,0,\ldots,0,0,1)$, $K_1 = (1,1,\ldots,1,1)$ et $K_2 = (0,1,1,\ldots,1,1,0)$ doit donner

$$(0,0,1,1,1,0,0,1,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0).$$

1. Attention : notre convention pour l'écriture binaire d'un nombre entier est que les bits de poids faible sont à droite. C'est le sens contraire des fonctions de conversions de Sage.

2 Calculer la matrice des approximations linéaires L de la boîte S de B32, c'est à dire la matrice de taille $2^4 \times 2^4$ contenant à l'entrée α, β le nombre

$$\mathrm{L}[\alpha,\beta] = \mathrm{Card}\{x \in (\mathbf{F}_2)^4, \alpha.x + \beta.\mathrm{S}(x) = 0\}$$

3 On choisit un couple (α,β) tel que la probabilité $p_{\alpha,\beta} = \mathrm{L}[\alpha,\beta]/2^4$ soit la plus éloignée de $1/2$. Par exemple $(\alpha,\beta) = (0100, 1000)$. Que vaut $p_{\alpha,\beta}$ dans ce cas ? De ce choix, déduire une équation linéaire reliant le message clair m et x_1 l'entrée du second (et dernier tour), du type $\mathrm{A}.m + \mathrm{B}.x_1 = 0$ et sa probabilité. Vérifier expérimentalement cette probabilité avec Sage (se donner des clefs de tours et tester avec un grand nombre de m aléatoires).

4 Récupérer une liste de couples clairs chiffrés disponibles à l'url :

`http://www.math.u-bordeaux1.fr/~gcastagn/Cryptanalyse/tp6-couples.sage`

Dans ce fichier pour `i` de 1 à 100, `Ciphertext[i]` est le chiffré de `Plaintext[i]`. On veut retrouver la clef K_2 de dernier tour utilisée lors du chiffrement.

Utiliser le couple $(\alpha,\beta) = (0100, 1000)$ qui permet d'avoir une seule boîte active au deuxième tour pour retrouver les bits 2 à 5 de la clef K_2. Pour cela pour chaque couple clair chiffré (m, c), faire une recherche exhaustive sur les bits 2 à 5 de la clef K_2 pour remonter partiellement le dernier tour et incrémenter un compteur correspondant à la clef utilisée si l'équation linéaire est vérifiée à l'entrée du dernier tour.

Utiliser également le couple $(\alpha,\beta) = (1010, 1011)$ qui donne deux boîtes actives.

5 Itérer l'attaque de la question précédente (avec une et deux boîtes actives) en « décalant » les équations linéaires pour avoir d'autres boîtes actives afin de déterminer les autres bits de K_2. Comparer l'efficacité de la méthode avec une boîte active et celle avec deux boîtes actives.

6 On suppose maintenant que B32 fait trois tours. Comment choisir l'équation linéaire pour que le nombre de boîtes actives à la fin du deuxième tour soit minimal ? Quelle est la probabilité correspondante ? Programmer cette attaque avec 3 tours et la tester en choisissant des clefs aléatoires $\mathrm{K}_0, \mathrm{K}_1, \mathrm{K}_2, \mathrm{K}_3$ et en construisant assez de couples clairs chiffrés correspondants.