Master CSI 2 2019-2020

Cryptanalyse — 4TCY902U
Responsable : G. Castagnos

TP 7 — Cryptanalyse linéaire et différentielle

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 $i \in \{0,\dots,15\}$ est identifiée avec son écriture binaire. Par exemple l'image de $[0,1,0,0]$ est donnée par $S[4] = 13$, c'est à dire $[1,1,0,1]$. Attention : on écrit ici un entier en binaire avec les bits de poids faible à droite. C'est le sens contraire des fonctions de conversions de Sage !

   On concatène les sorties des S-box pour obtenir 32 bits.

2. Permutation : Le bloc de 32 bits subit un décalage circulaire de 2 bits vers la droite ;

3. On ajoute la clé de tour (K_1 au premier et K_2 au second).

Récupérer le code Sage suivant, donnant la définition des fonctions de tour, de tour inverse, ainsi que le chiffrement complet à 2 tours avec 3 clés K_0, K_1, K_2 et la fonction de déchiffrement correspondante :

`https://www.math.u-bordeaux.fr/~gcastagn/Cryptanalyse/tp7-B32.sage`

I 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

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

2 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 $\langle \mathrm{A}, m\rangle \oplus \langle \mathrm{B}, x_1\rangle = 0$ et sa probabilité. Vérifier expérimentalement cette probabilité avec Sage (se donner des clefs de tours et tester avec un grand nombre de m aléatoires).

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

`https://www.math.u-bordeaux.fr/~gcastagn/Cryptanalyse/tp7-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.

4 Itérer l'attaque de la question précédente en « décalant » les équations linéaires pour avoir d'autres boîtes actives afin de déterminer les autres bits de K_2.

5 Calculer la matrice des différentielles de la boîte S de B32, c'est à dire la matrice de taille $2^4, 2^4$ contenant en l'entrée α, β le nombre

$$\mathrm{D}(\alpha, \beta) = \mathrm{Card}\Big\{(x, x^\star) \in \mathbf{F}_2^4 \times \mathbf{F}_2^4 \mid x \oplus x^\star = \alpha \text{ et } \mathrm{S}(x) \oplus \mathrm{S}(x^\star) = \beta\Big\},$$

où $\alpha, \beta \in \mathbf{F}_2^4$ sont identifiés avec les entiers de 0 à 15 pour les indices de positions dans la matrice.

6 On utilise la différentielle $(\alpha, \beta) = (0001, 0100)$ au niveau de la première S-box du premier tour. Soit $m, m^\star$ deux messages clairs, tel que $m \oplus m^\star = 00010 \ldots 0$. On note x_1 et $x_1^\star$, les blocs obtenus à l'entrée du dernier tour lors des chiffrements respectifs de m et $m^\star$. Avec quelle probabilité doit on avoir $x_1 \oplus x_1^\star = 00010 \ldots 0$?

7 Vérifier expérimentalement cette probabilité avec Sage (se donner des clefs de tours et tester avec un grand nombre de couples $(m, m^\star)$ aléatoires vérifiant $m \oplus m^\star = 00010 \ldots 0$).

8 Se donner des clefs de tours et construire cent couples de clairs vérifiant la différentielle $00010 \ldots 0$ et les couples de chiffrés correspondants. Retrouver les bits d'indices 2 à 5 de la clef K_2 à partir de ces chiffrés : 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 la différentielle $00010 \ldots 0$ est vérifiée à l'entrée du dernier tour.

9 Itérer l'attaque de la question précédente en « décalant » les différentielles pour avoir d'autres boîtes actives afin de déterminer les autres bits de K_2.