Cryptanalyse — 4TCY902U

Responsable : G. Castagnos

TP 7 — Cryptanalyse différentielle

On va attaquer le chiffrement B32 défini dans le projet avec la méthode de la cryptanalyse différentielle. On reprend les notations du projet.

1 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

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

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.

2 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 $x_1 \oplus x_1^\star = 00010 \ldots 0$?

3 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 $m \oplus m^\star = 00010 \ldots 0$).

4 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.

5 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.

6 Mêmes questions en utilisant la différentielle $(\alpha, \beta) = (1111, 1001)$ qui a une meilleure probabilité et qui donne deux boîtes actives.