Calcul sécurisé, Attaque par faute sur le DES

Niels Merceron
Numéro d'étudiant: 21801038

Table des matières

Chapitre 1

Attaque par faute sur le DES

1.1 Description du principe d'attaque par faute

On va injecté une faute a l'aide d'un laser dans un tour (dans notre cas le 15ème), de cette faute résultera un chiffré différent de celui sans faute. De ces Deux chiffrés on les comparera en effectuant divers calcul dessus pour arriver a manipulé quelque chose de simple et qui nous donne de l'information sur la clef secrète. Plus précissement, on identifera quel bit est touché par la faute. Une fois le bit identifié on regardera quel fontion sont touchées par ce bit fauté. Puis on effectura le calcul des fonctions touchés avec la version non fauté et fauté. Puis on comparera ces deux fonctions pour trouver des informations sur la clef secrète K .

Chapitre 2

Application concrète

2.1 Description de l'attaque par faute

On obtient donc comme partie de clef :

Chapitre 3

Retrouver la clef complète du DES

Pour retrouver les 8 bits manquants on peut force brute sur 2^8 valeur et calculer le Des avec chaque clef créé a l'aide des 2^8

On obtient donc comme clef :

Chapitre 4

Fautes sur les tours précédents

4.1 attaque sur le 14ème tour

4.2 attaque sur le 13ème tour

4.3 généralisation sur le nième tour

Chapitre 5

Contre-mesures

5.1 Doublé le calcul du DES

Une solution assez simple qui nous vient en tête est de calculé deux/plusieurs fois l'algorithme du DES pour le même message puis véfirier si les résultats obtenu a la fin est identique. Si les résultats sont identique alors il n'y a pas eu d'injection de faute, sinon une faute a été introduite on ne renvoie rien. Cependant cette méthode est partiellement efficace car on peut partir du principe que l'attaquant a plusieurs outils similaires pour faire la fautes au même endroit a chaque fois et donc que l'injection de faute soit un succès. Il faudrait donc calculer n+1 fois le DES (n étant le nombre d'outils qu'a l'attaquant) pour espérer s'en protéger ce qui donnerai une compléxité très grande. De plus si on voulais mettre cette solution dans une carte a puce on serait très vite limité au nombre de fois que l'ont puisse calculer le DES. La compléxité de cette solution serait de l'ordre K×O(DES), K étant le nombre de fois que l'ont calcul le DES.

5.2 rajouté de l'aléatoire/calcul imbriqué

Chapitre 6

Annexe