Calcul sécurisé - Contrôle continu

7 mars 2019

Table des matières

1 Question 1

Une attaque par faute contre le DES consiste à introduire une modification sur un bit du chiffré durant l'exécution du chiffrement. De ce fait si on dispose d'un chiffré correct et d'un chiffré fauté par l'attaque on peut obtenir des informations sur la clé utilisée pour le chiffrement. En supposant que l'attaquant est capable d'effectuer une faute sur la valeur de sortie R15 du 15ème tour une attaque par faute peut être décrite de la façon suivante :
On suppose que l'erreur correspond est induite en effectuant l'operation XOR entre la valeur R14 et un E aléatoire de la taille de R14.
On obtient ainsi R14 XOR E = R14*. Au tour suivant on aura donc :
L15 = R14* = L15*
R15 = L14 XOR f(R14*) = R15 XOR e' = R15*.
Au dernier tour L16 = R15* = R16* et R16 = L15* = R14*.
Après une dernière permutation P^{-1} on obtient finalement le chiffré C XOR x = C*.
Si on a également un chiffré C non fauté alors on va pouvoir retrouver la sous-clé K15 utilisée par la fonction F pour R14 et à partir de la retrouver la clé K utilisée pour le chiffrement du message.

2 Question 2

2.1 Décrire précisément ce que vous faites pour retrouver la clé

2.2 Donnez les 48 bits de clé que vous obtenez grâce à cette attaque par fautes

3 Question 3

3.1 Expliquer comment on peut retrouver les 8 bits manquants

3.2 Faites-le, et donner ainsi la valeur complète de la clé qui vous a été assignée.

4 Question 4

5 Question 5