Calcul sécurisé - Attaque par faute sur DES

CAUMES Clément 21501810

Master 1 Informatique SeCReTs

1 Question 1 : Attaque par faute sur le DES

Une attaque par faute consiste à changer le résultat d'un sous calcul afin d'obtenir une information secrète. Ce changement va donc produire volontairement une erreur. Cette attaque est physique car, pour modifier la valeur de certains bits, il est nécessaire d'agir physiquement sur les composants électroniques. Dans le cas du DES avec une attaque par faute sur la valeur de sortie R_{15} du 15^e tour, cela signifie que la valeur R_{15} va être changer par l'attaquant.

[mettre une image]

A partir de cette attaque, il est possible de retrouver la clé secrète utilisée par la victime à partir de la sous clé K_{15}. On suppose ici que nous sommes l'attaquant et que nous avons réussi à obtenir de la victime le message clair associé à son message chiffrée (avec une clé inconnue pour le moment, qui est à trouver). De plus, nous avons eu de la victime 32 chiffrés (toujours avec la même clé) et dont on a réussi à faire une attaque par faute.

2 Question 2 : Application concrète

1. Cette attaque par faute sur le dernier tour du DES comporte plusieurs étapes :

— étape 1 : trouver R_{15} à partir du chiffré juste et les $R_{15}*$ à partir des chiffrés faux.
Pour cela, on fait une permutation initiale (qui annule la permutation finale IP^{-1}) pour trouver L_{16} et R_{16}. On fera de même pour $R_{15}*$ à partir des chiffrés faux. On peut désormais écrire les formules suivantes :

$R_{16} = L_{15} \oplus f(K_{16}, R_{15})$ et $L_{16} = R_{15}$ pour le chiffré juste.
$R_{16}* = L_{15} \oplus f(K_{16}, R_{15}*)$ et $L_{16}* = R_{15}*$ pour les chiffrés faux.

Le but ici est d'obtenir K_{16} : pour cela, on fait le XOR entre R_{16} et un $R_{16}*$. Ce qui nous donne l'équation suivante :

$R_{16} \oplus R_{16}* = L_{15} \oplus f(K_{16}, R_{15}) \oplus L_{15} \oplus f(K_{16}, R_{15}*)$
Les L_{15} s'annulent et on obtient : $R_{16} \oplus R_{16}* = f(K_{16}, R_{15}) \oplus f(K_{16}, R_{15}*)$

Or, $f(K_{i+1}, R_i) = P(S(E(R_i) \oplus K_{i+1})) = P(S_1(E(R_i) \oplus K_{i+1})_{b_1 \to b_6} || ... || S_8(E(R_i) \oplus K_{i+1})_{b_{43} \to b_{48}})$

— étape 2 : pour chaque chiffré faux (associé à son $R_{15}*$), établir 8 équations pour chaque boîte-S.

$P^{-1}(R_{16} \oplus R_{16}*)_{b_1 \to b_4} = S_1(E(R_{15}) \oplus K_{16})_{b_1 \to b_4} \oplus S_1(E(R_{15}*) \oplus K_{16})_{b_1 \to b_4}$
$P^{-1}(R_{16} \oplus R_{16}*)_{b_5 \to b_8} = S_1(E(R_{15}) \oplus K_{16})_{b_5 \to b_8} \oplus S_1(E(R_{15}*) \oplus K_{16})_{b_5 \to b_8}$
$P^{-1}(R_{16} \oplus R_{16}*)_{b_9 \to b_{12}} = S_1(E(R_{15}) \oplus K_{16})_{b_9 \to b_{12}} \oplus S_1(E(R_{15}*) \oplus K_{16})_{b_9 \to b_{12}}$
$P^{-1}(R_{16} \oplus R_{16}*)_{b_{13} \to b_{16}} = S_1(E(R_{15}) \oplus K_{16})_{b_{13} \to b_{16}} \oplus S_1(E(R_{15}*) \oplus K_{16})_{b_{13} \to b_{16}}$
$P^{-1}(R_{16} \oplus R_{16}*)_{b_{17} \to b_{20}} = S_1(E(R_{15}) \oplus K_{16})_{b_{17} \to b_{20}} \oplus S_1(E(R_{15}*) \oplus K_{16})_{b_{17} \to b_{20}}$
$P^{-1}(R_{16} \oplus R_{16}*)_{b_{21} \to b_{24}} = S_1(E(R_{15}) \oplus K_{16})_{b_{21} \to b_{24}} \oplus S_1(E(R_{15}*) \oplus K_{16})_{b_{21} \to b_{24}}$
$P^{-1}(R_{16} \oplus R_{16}*)_{b_{25} \to b_{28}} = S_1(E(R_{15}) \oplus K_{16})_{b_{25} \to b_{28}} \oplus S_1(E(R_{15}*) \oplus K_{16})_{b_{25} \to b_{28}}$
$P^{-1}(R_{16} \oplus R_{16}*)_{b_{29} \to b_{32}} = S_1(E(R_{15}) \oplus K_{16})_{b_{29} \to b_{32}} \oplus S_1(E(R_{15}*) \oplus K_{16})_{b_{29} \to b_{32}}$

— étape 3 : éliminer les équations dont $(R_{16} \oplus R_{16}*)_{b_x \to b_y}$ s'annulent.
— étape 4 : faire une attaque exhaustive sur le contenu