

# Calcul sécurisé - Attaque par faute sur DES

CAUMES Clément 21501810

Master 1 Informatique SeCReTs

## Table des matières

1	Question 1 : Attaque par faute sur le DES	3
2	Question 2 : Application concrète	3

## 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<sup>e</sup> 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 :

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

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 :  $R_{16} \oplus R_{16}^* = f(K_{16}, R_{15}) \oplus f(K_{16}, R_{15}^*)$

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

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

$$P^{-1}(R_{16} \oplus R_{16}^*)_{b_1 \rightarrow b_4} = S_1(E(R_{15}) \oplus K_{16})_{b_1 \rightarrow b_4} \oplus S_1(E(R_{15}^*) \oplus K_{16})_{b_1 \rightarrow b_4}$$
$$P^{-1}(R_{16} \oplus R_{16}^*)_{b_5 \rightarrow b_8} = S_2(E(R_{15}) \oplus K_{16})_{b_5 \rightarrow b_8} \oplus S_2(E(R_{15}^*) \oplus K_{16})_{b_5 \rightarrow b_8}$$
$$P^{-1}(R_{16} \oplus R_{16}^*)_{b_9 \rightarrow b_{12}} = S_3(E(R_{15}) \oplus K_{16})_{b_9 \rightarrow b_{12}} \oplus S_3(E(R_{15}^*) \oplus K_{16})_{b_9 \rightarrow b_{12}}$$
$$P^{-1}(R_{16} \oplus R_{16}^*)_{b_{13} \rightarrow b_{16}} = S_4(E(R_{15}) \oplus K_{16})_{b_{13} \rightarrow b_{16}} \oplus S_4(E(R_{15}^*) \oplus K_{16})_{b_{13} \rightarrow b_{16}}$$
$$P^{-1}(R_{16} \oplus R_{16}^*)_{b_{17} \rightarrow b_{20}} = S_5(E(R_{15}) \oplus K_{16})_{b_{17} \rightarrow b_{20}} \oplus S_5(E(R_{15}^*) \oplus K_{16})_{b_{17} \rightarrow b_{20}}$$
$$P^{-1}(R_{16} \oplus R_{16}^*)_{b_{21} \rightarrow b_{24}} = S_6(E(R_{15}) \oplus K_{16})_{b_{21} \rightarrow b_{24}} \oplus S_6(E(R_{15}^*) \oplus K_{16})_{b_{21} \rightarrow b_{24}}$$
$$P^{-1}(R_{16} \oplus R_{16}^*)_{b_{25} \rightarrow b_{28}} = S_7(E(R_{15}) \oplus K_{16})_{b_{25} \rightarrow b_{28}} \oplus S_7(E(R_{15}^*) \oplus K_{16})_{b_{25} \rightarrow b_{28}}$$
$$P^{-1}(R_{16} \oplus R_{16}^*)_{b_{29} \rightarrow b_{32}} = S_8(E(R_{15}) \oplus K_{16})_{b_{29} \rightarrow b_{32}} \oplus S_8(E(R_{15}^*) \oplus K_{16})_{b_{29} \rightarrow b_{32}}$$

— étape 3 : éliminer les équations dont  $P^{-1}(R_{16} \oplus R_{16}^*)_{b_x \rightarrow b_y}$  s'annulent.

— étape 4 : faire une attaque exhaustive sur les sorties de chaque boîte-S. Cela permettra d'obtenir plusieurs cas possibles pour les entrées de celle-ci. En effet, il y a plusieurs solutions possibles pour la

sortie d'une boîte-S, sachant qu'elles ne sont pas linéaires. De ce fait, on récupère toutes les solutions possibles pour chaque boîte-S. Une solution commune sera présente pour chaque chiffré faux qui sera la portion de bits de  $K_{16}$ .