Calcul sécurisé - Attaque par faute sur DES

CAUMES Clément 21501810

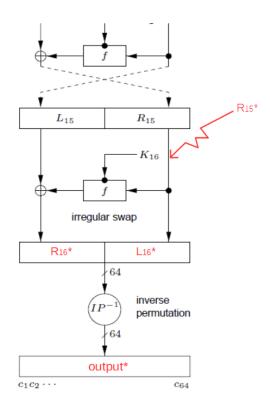
Master 1 Informatique SeCReTs

Table des matières

1	Question 1 : Attaque par faute sur le DES	3
2	Question 2 : Application concrète	3
3	Ouestion 3 : Retrouver la clé complète du DES	4

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.



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}})
```

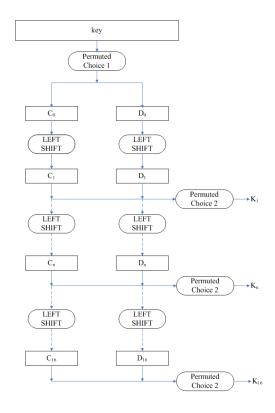
— étape 2 : pour chaque chiffré faux (associé à son $R_{15}*$), établir 8 équations pour chaque boîte-S.

```
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_{2}(E(R_{15}) \oplus K_{16})_{b_{5}\to b_{8}} \oplus S_{2}(E(R_{15}*) \oplus K_{16})_{b_{5}\to b_{8}}
P^{-1}(R_{16} \oplus R_{16}*)_{b_{9}\to b_{12}} = S_{3}(E(R_{15}) \oplus K_{16})_{b_{9}\to b_{12}} \oplus S_{3}(E(R_{15}*) \oplus K_{16})_{b_{9}\to b_{12}}
P^{-1}(R_{16} \oplus R_{16}*)_{b_{13}\to b_{16}} = S_{4}(E(R_{15}) \oplus K_{16})_{b_{13}\to b_{16}} \oplus S_{4}(E(R_{15}*) \oplus K_{16})_{b_{13}\to b_{16}}
P^{-1}(R_{16} \oplus R_{16}*)_{b_{17}\to b_{20}} = S_{5}(E(R_{15}) \oplus K_{16})_{b_{17}\to b_{20}} \oplus S_{5}(E(R_{15}*) \oplus K_{16})_{b_{17}\to b_{20}}
P^{-1}(R_{16} \oplus R_{16}*)_{b_{21}\to b_{24}} = S_{6}(E(R_{15}) \oplus K_{16})_{b_{21}\to b_{24}} \oplus S_{6}(E(R_{15}*) \oplus K_{16})_{b_{21}\to b_{24}}
P^{-1}(R_{16} \oplus R_{16}*)_{b_{25}\to b_{28}} = S_{7}(E(R_{15}) \oplus K_{16})_{b_{25}\to b_{28}} \oplus S_{7}(E(R_{15}*) \oplus K_{16})_{b_{29}\to b_{32}}
P^{-1}(R_{16} \oplus R_{16}*)_{b_{29}\to b_{32}} = S_{8}(E(R_{15}) \oplus K_{16})_{b_{29}\to b_{32}} \oplus S_{8}(E(R_{15}*) \oplus K_{16})_{b_{29}\to b_{32}}
```

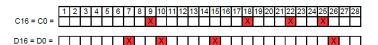
- étape 3 : éliminer les équations dont $P^{-1}(R_{16} \oplus R_{16}*)_{b_x \to b_y}$ s'annulent. [ATTENTION SI SX() XOR SX() vaut 0 aussi]
- étape 4 : faire une attaque exhaustive sur les sorties de chaque boîte-S. Cela permettra d'obtenir plusieurs cas possibles pour les entrées de celle-ci. En effet, 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} .

3 Question 3 : Retrouver la clé complète du DES

1. Dans la question précédente, nous avons réussi à obtenir la clé secrète K_{16} qui contient 48 bits. En analysant le schéma de création des 16 sous-clés (de 48 bits) à partir de la clé secrète (de 56 bits), on peut en déduire la clé secrète. Cela comporte plusieurs étapes :



— étape 1 : effectuer une permutation inverse $PC_2^{-1}(K_{16})$ afin d'obtenir C_{16} et D_{16} . Il est important de noter que lors de cette permutation inverse, 8 bits sont inconnus. En effet, on passe de 48 bits à $2 \times 28 = 56$ bits. Il y a donc 8 bits qu'on ne peut déduire à partir de K_{16} .



Sur ce schéma, les bits encore inconnus sont marqués par "X".

- étape 2 : Déduire C_0 et D_0 à partir de C_{16} et D_{16} . En effet, $C_0 = C_{16}$ et $D_0 = D_{16}$ puisque la somme des shifts circulaires donne 28 qui correspond à la taille des blocs C_i et D_i . Les 8 bits inconnus n'ont donc pas bougé de place dans C_0 et D_0 .
- étape 3 : Effectuer une permutation inverse $PC_1^{-1}(C_0||D_0)$ afin d'obtenir la clé finale sur 64 bits. On peut noter ici que les 8 bits inconnus sont mélangés dans la clé finale. De plus, 8 bits supplémentaires ont été rajoutés correspondant aux bits de parité. On a donc une clé finale sur 64 bits dont 16 bits sont inconnus.



Sur le schéma ci-dessous, "B" correspond aux bits de parité.

- étape 4 : Retrouver les 8 bits inconnus par une recherche exhaustive : $2^8 = 256$ cas possibles. Pour chaque clé possible, on faire le chiffrement DES avec en entrée la clé possible et le message clair fourni. Si la clé testée est celle recherchée, alors le chiffré obtenu sera identique à celui du chiffré correct fourni.
- étape 5 : déduire les 8 bits de parité en s'assurant que chaque octet possède un nombre impair de bits à 1.
- 2. On va effectuer les différentes étapes en détaillant :

— On a obtenu précédemment lors de la recherche de la sous clé : $K_{16}=02\ 10\ B1\ 2C\ 47\ 79.$

Avec l'étape 1 et 2, on obtient :

- $C_0 = C_{16} = 0110\ 00100100\ 00010000\ 00000100 = 6241004$
- $D_0 = D_{16} = 0011\ 00000010\ 01001110\ 11001011 = 3024 ECB$
- $C_0||D_0 = 62\ 41\ 00\ 43\ 02\ 4E\ CB$

Les 8 bits inconnus à chercher sont à 0.

- Avec l'étape 3, on obtient la clé DES sur 64 bits avec les 8 bits inconnus à 0 et les bits de parité également à 0 :
 - K_{64} * = 50 90 0C 18 02 8E D8 08
- On réalise l'attaque exhaustive et on trouve la solution en ajustant également les bits de parité et on obtient la solution finale de la clé DES sur 64 bits en hexadécimal :

 $K_{64} = 51 \ 92 \ 2C \ 19 \ 02 \ 8F \ FD \ 49$