

# Calcul sécurisé, Attaque par faute sur le DES

Niels Merceron  
Numéro d'étudiant: 21801038

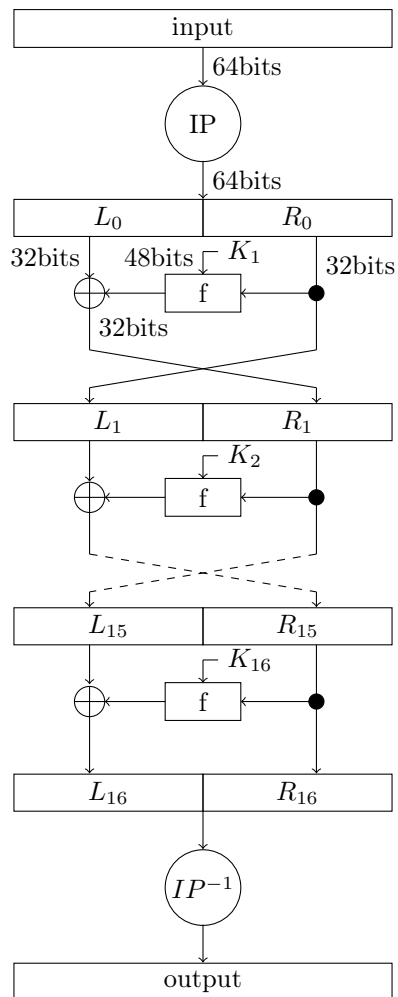


# Table des matières

<b>1</b>	<b>Attaque par faute sur le DES</b>	<b>2</b>
1.1	Description du principe d'attaque par faute . . . . .	3
<b>2</b>	<b>Application concrète</b>	<b>4</b>
2.1	Description de l'attaque par faute . . . . .	4
<b>3</b>	<b>Retrouver la clef complète du DES</b>	<b>7</b>
<b>4</b>	<b>Fautes sur les tours précédents</b>	<b>8</b>
4.1	attaque sur le 14ème tour . . . . .	8
4.2	attaque sur le 13ème tour . . . . .	8
4.3	généralisation sur le nième tour . . . . .	8
<b>5</b>	<b>Contre-mesures</b>	<b>9</b>
5.1	Doublé le calcul du DES . . . . .	9
5.2	Diffusion de l'erreur . . . . .	9
<b>6</b>	<b>Annexe</b>	<b>10</b>

# 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 identifiera 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

Pour commencer on veut obtenir R16 et L16 donc on effectue au chiffé correcte les permutations décrite par IP. On fait la même chose pour obtenir R16' et L16' qui correspondent au chiffé fauté.

On a donc  $R_{16} = R_{15}$ ,  $L_{16} = L_{15} \oplus f(R_{15}, K_{16})$  mais aussi  $R'_{16} = R'_{15}$  et  $L'_{16} = L_{15} \oplus f(R'_{15}, K_{16})$ . Pour savoir où se situe l'erreur on effectue le calcul suivant  $R_{16} \oplus R'_{16} = R_{15} \oplus R'_{15} = R_{15} \oplus R_{15} \oplus \mathcal{E} = \mathcal{E}$ . Savoir où se situe l'erreur nous aidera plus tard.

Une fois cela fait on passe à la partie plus technique. Notre but est de trouver une formule avec ce que nous connaissons, avec K16 dedans et la plus réduite possible. On va donc commencer par effectuer :

$$L'_{16} \oplus L_{16} = L_{15} \oplus F(R'_{15}, K_{16}) \oplus L_{15} \oplus F(R_{15}, K_{16}) = F(R'_{15}, K_{16}) \oplus F(R_{15}, K_{16}).$$

une fois cela fait on va écrire explicitement la fonction F. Cette fonction F consiste en une expansion(E) puis on xor le résultat avec  $K_i$  (dans notre cas  $K_{16}$ ) ensuite le résultat du xor passe dans les Sbox et pour finir passe dans une permutation(P).

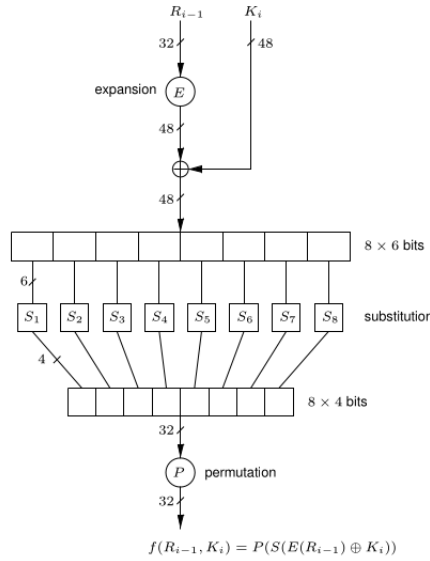


Schéma de la fonction F

on obtient donc la formule suivant :

$$L'_{16} \oplus L_{16} = P(S(E(R'_{15}) \oplus K_{16})) \oplus P(S(E(R_{15}) \oplus K_{16}))$$

De cette formule on peut enlever la permutation P car on connais l'empla-  
cement des bits permuté et la permutaion P est linéaire.

on a donc :

$$P^{-1}(L'_{16} \oplus L_{16}) = P^{-1}(P(S(E(R'_{15}) \oplus K_{16})) \oplus P(S(E(R_{15}) \oplus K_{16})))$$

$$P^{-1}(L'_{16} \oplus L_{16}) = S(E(R'_{15}) \oplus K_{16}) \oplus S(E(R_{15}) \oplus K_{16})$$

A ce stade on ne peut pas réduire plus cette formule car S est non linéaire  
donc je ne peux pas l'enlever comme j'ai fait avec la permutation P.

On va nommer deux variable  $\alpha = E(R_{15}) \oplus K_{16}$  et  $\alpha' = E(R'_{15}) \oplus K_{16}$ . Par force  
brute on va déterminer tous les  $\alpha'$  passant dans la sbx nous donnant les même  
bits de sorti avant permutation. Cela représente une force brute sur  $2^6$  valeurs a  
tester. On effectuera cette tache pour chaque chiffré fauté en notre possession.

Je vais étendre les  $\alpha'$  obtenu jusqu'a 48bits pour pouvoir effectuer les calculs  
suivant tout en gardant l'emplacement de alpha parmi les 48bits rajouter.

$R'_{15}$  est connu ( $R'_{16} = R'_{15}$ ) donc je vais calculer l'expansion de  $R'_{15}$  puis effectuer  
un xor entre cette expansion et les  $\alpha'$  déterminer précédement. De faire ce calcul  
me permettra d'avoir 6 bit de la clef  $K_{16}$  cependant j'aurai plusieurs candidats  
(noté  $\gamma$ ) car j'ai plusieurs  $\alpha'$ .

Dans un premier temps pour déterminer le bon candidat je vais calculer  $\alpha$  avec  
comme clé un  $\gamma$  a l'emplacement de la sbx touché par la faute ce qui nous  
donnera une clef de 48 bits. j'effectuerai cette opération autant de fois qu'il y a  
de  $\gamma$ .

Dans un second temps, je passerai le résultat de  $\alpha$  dans les sbx puis je vérifie  
que le résultat obtenu est le bon avant permutation. Si il est bon alors cela veut  
dire que j'ai trouvé les 6 bon bits de clef ( $\gamma$ ) sinon je continue jusqu'a trouver

le bon  $\gamma$  me donnant la bonne sortie avant permutation.

Exemple : la faute est situé au 30ème bit.

on a donc :

$$S(E(R_{15}) \oplus K_{16}) = 01 \dots 1010 \ 1110$$

$$E(R'_{15}) = 10 \dots 1001 \ 0110$$

$$\alpha'_1 = 00 \dots 0010 \ 0111$$

$$\alpha'_2 = 00 \dots 0001 \ 0100$$

$$\gamma_1 = E(R'_{15}) \oplus \alpha'_1 = 10 \dots 1011 \ 0001$$

$$\gamma_2 = E(R'_{15}) \oplus \alpha'_2 = 10 \dots 1000 \ 0010$$

$\alpha_{\gamma_1} = 01 \dots 1000 \ 0101$ ,  $\alpha_{\gamma_1}$  n'est pas le bon candidat car les 4 derniers bits sont différent de celui de  $S(E(R_{15}) \oplus K_{16})$ .

$\alpha_{\gamma_2} = 00 \dots 0110 \ 1110$ ,  $\alpha_{\gamma_2}$  les 4 derniers bit sont équivalent à  $S(E(R_{15}) \oplus K_{16})$  donc les bit de 31 à 28 sont égaux a ceux de  $\gamma_2$ .

Pour finir après avoir appliquer l'attaque décrite un peu plus haut j'obtiens la clef suivante : B1A6E1869A35

## Chapitre 3

# Retrouver la clef complète du DES

Pour retrouver 48bits des 56bits de la clef j'effectue le cadencement de clef a l'inverse de comment il est décrit. Une fois ces 48 bits déterminer, certains bits n'ont pas de valeurs donc pour retrouver ces derniers 8 bits on va les faire varier en effectuant une force brute de  $2^8$  valeurs. A chaque valeur on effectue le DES avec la nouvelle clef, tant que nous obtenons pas le bon chiffré en sorti on continue de faire varier les 8bits manquants. Une fois le bon chiffré en sorti, la bonne clef de 56 bits a été trouvé.

On obtient donc comme clef : E65875255B64BA40



## 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 vérifier si les résultats obtenus à la fin est identique. Si les résultats sont identiques 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 à 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 complexité très grande. De plus si on voulait mettre cette solution dans une carte à puce on serait très vite limité au nombre de fois que l'ont puisse calculer le DES. La complexité de cette solution serait de l'ordre  $K \times O(\text{DES})$ ,  $K$  étant le nombre de fois que l'ont calcul le DES.

### 5.2 Diffusion de l'erreur

Une autre solution que j'ai discuté avec mon chargé de td est la diffusion de l'erreur. Plus précisément, le but est de propagé l'erreur à tous les bits, plusieurs fois de manière non linéaire pour que le chiffré obtenu par l'attaquant ne puisse lui donner aucune information sur la clef ou tout autre élément utile à l'attaquant. Cependant dans les fait cette solution n'a pas encore été réalisé pour le DES ou autre chiffrement du même type que le DES. Il y a un problème majeur avec cette méthode il faut déjà détecter la faute ce qui n'est pas trop compliqué en soit mais de cette détection découle le fait d'appliquer ou non la diffusion de la faute. A énoncé verbalement c'est simple mais dans les faits aucun modèle ou solution concrète n'a été décrite à ce jour dans la littérature Cryptographique.

## Chapitre 6

## Annexe