Contrôle continu

Malek Zemni

Attaque par faute sur DES

03/04/2018

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES
université PARIS-SACLAY

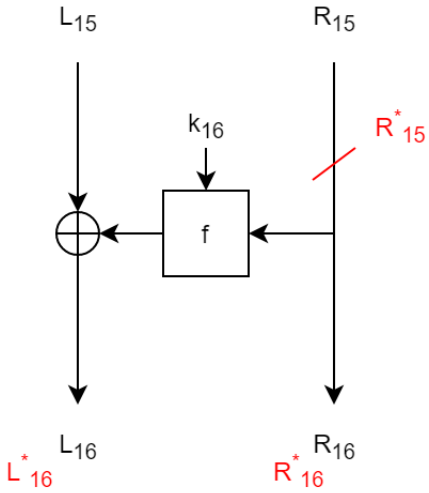
Calcul sécurisé

Question 1 :

Description d'une attaque par faute contre le DES sur la sortie R_{15} du 15ème tour.

L'attaque par faute contre le DES est une attaque provoquant une faute intentionnelle dans l'algorithme afin de compromettre ses calculs. Cette faute va permettre de révéler une partie de la clé utilisée. Une attaque par recherche exhaustive sur la clé du DES a une complexité de 2^{56}. L'objectif de l'attaque par faute est donc d'accélérer la recherche.

Dans notre cas, la faute est provoquée à la sortie R_{15} du 15ème tour de Feitsel du DES. Il s'agit d'un échange d'un seul bit parmi les 32 bits de R_{15} (*single bit flip*), ce qui va donner une sortie fausse au 15ème tour qu'on note R^*_{15}. La figure ci-dessous illustre l'injection d'une faute à la sortie 15ème tour du DES :



Pour exploiter cette faute, on va analyser les résultats obtenus à la sortie du 16ème tour. On a :

— $L_{16} = L_{15} \oplus f(R_{15}, k_{16})$

— $R_{16} = R_{15}$

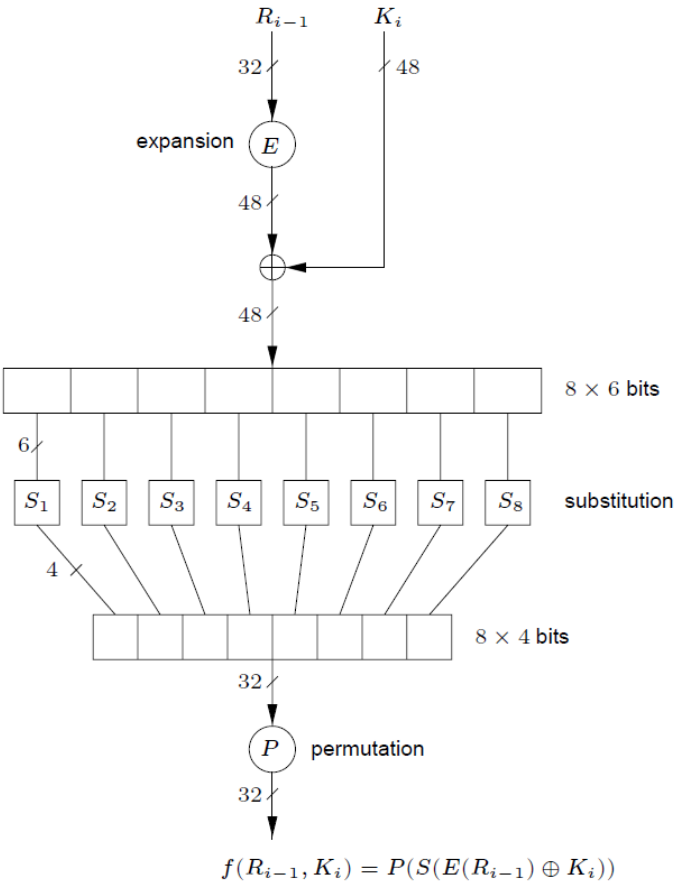
— $L^*_{16} = L_{15} \oplus f(R^*_{15}, k_{16})$

— $L^*_{16} = R^*_{15}$

On remarque que L_{16} et L^*_{16} font toutes les deux intervenir la clé k_{16} qui est l'objet initial de cette attaque. On exploite donc L_{16} et L^*_{16} pour construire une équation permettant de retrouver k_{16}. On effectue un XOR entre L_{16} et L^*_{16} pour éliminer L_{15}, l'équation obtenue est donc :

$$L_{16} \oplus L^*_{16} = f(R_{15}, k_{16}) \oplus f(R^*_{15}, k_{16})$$

On va maintenant s'intéresser à la fonction interne f du DES afin de mieux exploiter l'équation obtenue précédemment. Cette fonction est illustrée par la figure ci-dessous :



L'analyse de cette fonction nous permet d'établir que :

— $f(R_{15}, k_{16}) = P[\quad S_1(E(R_{15}) \oplus k_{16\ \text{bits}\ 1\to6}) \quad || \ldots || \quad S_8(E(R_{15}) \oplus k_{16\ \text{bits}\ 43\to48}) \quad]$

— $f(R^*_{15}, k_{16}) = P[\quad S_1(E(R^*_{15}) \oplus k_{16\ \text{bits}\ 1\to6}) \quad || \ldots || \quad S_8(E(R^*_{15}) \oplus k_{16\ \text{bits}\ 43\to48}) \quad]$

En effet, la fonction f prend en entré le demi-bloc R de 32 bits auquel elle applique une expansion de 48 bits, ainsi que la clé k_{16}. Ces deux entrées sont mélangées à l'aide d'un XOR pour obtenir une entité de 48 bits. Ces 48 bits vont être répartis sur 8 boites de substitution appelées *S-box*. Chacune des 8 S-box prend 6 bits en entrée et en renvoie 4, pour avoir un résultat final de 32 bits. Ces S-box vont être l'objet principal de l'attaque. L'équation précédemment établie devient ainsi :

$$L_{16} \oplus L^*_{16} = f(R_{15}, k_{16}) \oplus f(R^*_{15}, k_{16})$$

$$\Leftrightarrow$$

$$L_{16} \oplus L^*_{16}$$

$$=$$

$$P\ [\ S_1(E(R_{15}) \oplus k_{16\ \text{bits}\ 1\to6}) \quad || \ldots || \quad S_8(E(R_{15}) \oplus k_{16\ \text{bits}\ 43\to48})\ ]$$

$$\oplus$$

$$P\ [\ S_1(E(R^*_{15}) \oplus k_{16\ \text{bits}\ 1\to6}) \quad || \ldots || \quad S_8(E(R^*_{15}) \oplus k_{16\ \text{bits}\ 43\to48})\ ]$$

En appliquant l'inverse de la permutation P (calculée à la main en prenant le chemin inverse de la permutation P fournie dans la documentation du DES), et en s'appuyant la propriété d'une permutation P quelconque, $P(a \oplus b) = P(a) \oplus P(b)$, on obtient :

$$P^{-1}(L_{16} \oplus L^*_{16})$$

$$=$$

$$S_1\ (E(R_{15}) \oplus k_{16\ \text{bits}\ 1\to6}) \quad \oplus \quad S_1\ (E(R^*_{15}) \oplus k_{16\ \text{bits}\ 1\to6})$$

$$||\ \ldots\ ||$$

$$S_8\ (E(R_{15}) \oplus k_{16\ \text{bits}\ 43\to48}) \quad \oplus \quad S_8\ (E(R^*_{15}) \oplus k_{16\ \text{bits}\ 43\to48})$$

Finalement, en répartissant cette équation sur les 8 S-box, on obtient 8 équations dont les membres font 4 bits et les solutions font 6 bits :

— $P^{-1}(L_{16} \oplus L^*_{16})_{\ \text{bits}\ 1\to4} = S_1\ (E(R_{15}) \oplus k_{16})_{\ \text{bits}\ 1\to4} \oplus S_1\ (E(R^*_{15}) \oplus k_{16})_{\ \text{bits}\ 1\to4}$

— ...

— $P^{-1}(L_{16} \oplus L^*_{16})_{\ \text{bits}\ 29\to32} = S_8\ (E(R_{15}) \oplus k_{16})_{\ \text{bits}\ 29\to32} \oplus S_8\ (E(R^*_{15}) \oplus k_{16})_{\ \text{bits}\ 29\to32}$

La seule inconnue dans toutes ces équations est k_{16}. Pour trouver k_{16}, il faut faire une recherche exhaustive sur chacune des 8 S-box correspondant à chacune des 8 équations. Chaque recherche sur les S-box va permettre de révéler 6 bits de k_{16}, pour en avoir au final 48 bits. La complexité de cette attaque est donc de 8 x 2^6.

Question 2

2.1 Recherche de la clé k_{16} de 48 bits

Remarque : les manipulations décrites dans cette partie sont implémentées dans le fichier source `DES_K16.c`.