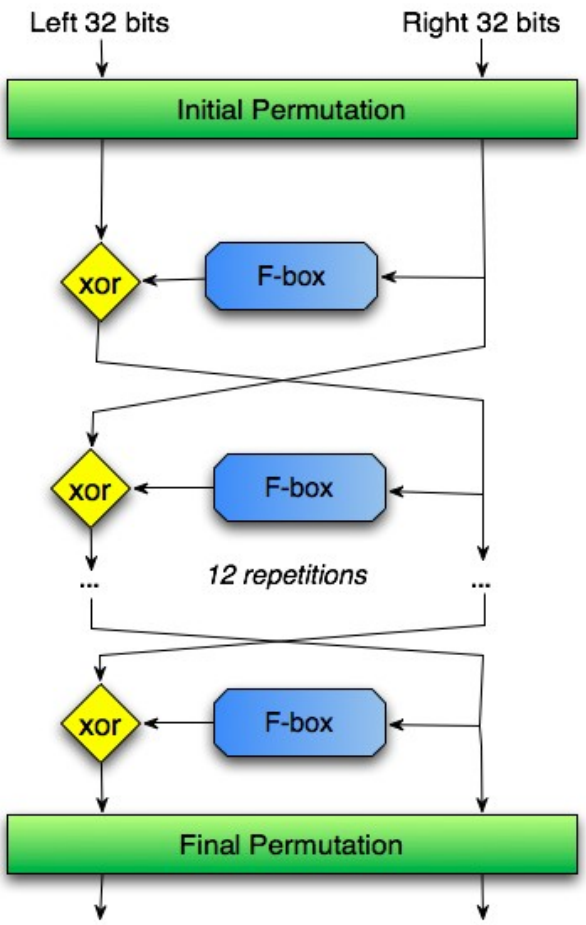
Rapport De Projet

Attaque par faute sur DES

Slimani Arezki 21502933



Question 1 :

Description De l'attaque par faute contre le DES :

L'attaque par faute contre le DES est l'une des attaques qui permet d'obtenir la clef de chiffrement d'un message chiffré, sa particularité est qu'il est plus rapide que certain algorithme de recherche tel que la recherche exhaustive qui a une complexité dans le pire des cas de 2^{56} (la clef fait 64 bit dont 8 bits de parité, donc 56 bits utiliser).

Le concept de l'attaque par faute sur le DES consiste a perturber le comportement du circuit afin de modifier l'exécution correcte du chiffrement. Les fautes son injecter dans le circuit par différents moyens tel que : le laser (sur les cartes a puces), des impulsions lumineuses, la perturbation de l'alimentation, champs magnétiques etc.

Passons maintenant a la pratique. On suppose que l'attaquant est capable d'effectuer une faute sur la valeur de sortie R_{15} du 15^e tour de Feistel. Concrètement cela veut dire que l'attaquant doit changer un seul bit parmi les 32 bits de R_{15}, et celui ci doit procéder de cette manière pour les 32 bits, Observons de plus près ce qu'induit l'injection d'une faute à la sortie de R_{15} qu'on notera R^*_{15}(voir le schéma 1):

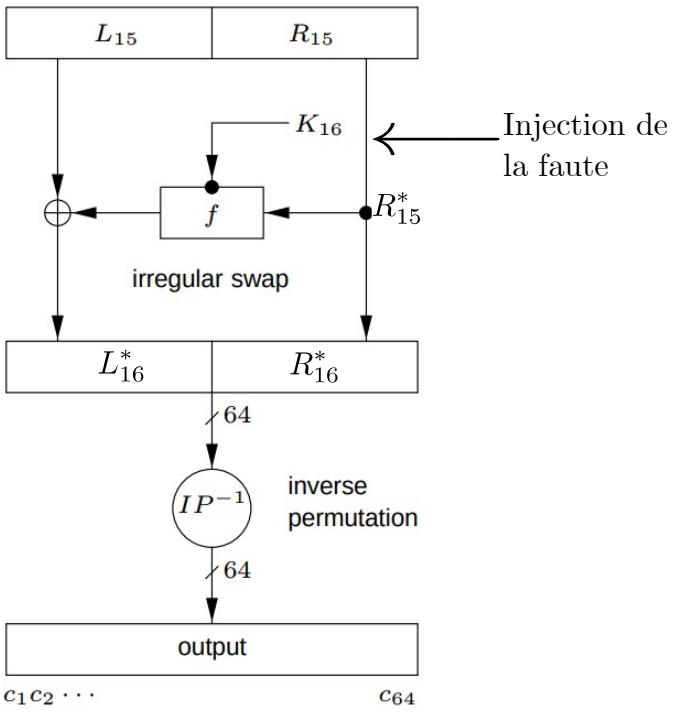


schéma 1: Insertion d'une faute sur R_{15}

Comme vous pouvez le remarquer sur le schéma 1, l'injection de la faute sur R_{15} a induit une faute sur R^*_{16} et L^*_{16}, passons maintenant à la partie mathématique et regardons ce que l'injection de faute nous permet d'avoir comme information, essayant de comparer les sorties obtenue avec et sans injection de faute :

1) sans injection de faute :

- $\triangleright\ R_{16} = R_{15}$
- $\triangleright\ L_{16} = L_{15} \oplus f(R_{15}, K_{16})$

2) avec injection de faute :

- $\triangleright\ R^*_{16} = R^*_{15}$
- $\triangleright\ L^*_{16} = L_{15} \oplus f(R^*_{15}, K_{16})$

Si on analyse bien ces deux cas, on vois bien que la partie qui nous permettrai d'obtenir un jour la clef K_{16} est celle de gauche gauche (avec L_{16} et L^*_{16}) car la clef K_{16} n'apparaît que dans ces deux équations. Si on analyse bien L_{16} et L^*_{16} on peut remarquer que L_{15} apparaît dans les deux, donc dans un premier temps, nous allons essayer de le faire disparaître de l'équation, pour cela nous devant faire un XOR de L_{16} et L^*_{16}