TP Attaque CPA sur RSA

Réalisé par :

FAHD LYOUSFI

Introduction :

Le TP se compose d'un microcontrôleur qui exécute un algorithme « Baby RSA » pour chiffrer des messages. Le « Baby RSA » utilise une exponentiation modulaire avec le parcours de l'exposant de gauche à droite suivant l'algorithme :

```
M_d_mod_N(M,d,N)
        T :=M
        For(i=len(d)-2 ;i<=0 ;i--)
                T:=T² mod N
                If(d[i]==1)
                        T:=T*M mod N
                End If
        End For
End
```

Figure 1 - Algorithme de l'exponentiation modulaire

Le but de TP est de retrouver la clé privée par une attaque des canaux cachées. En préalable, 1000 messages connus étaient chiffrés par une clé privée inconnue dont les traces des consommations électriques étaient mesurées et enregistrées.

L'attaque :

L'attaque exécutée est une attaque de type CPA (Correlation Power Analysis) vu les données disponibles. L'idée est de calculer le Hamming Weight du résultat de l'exponentiel modulaire de chaque message en rajoutant Bit par Bit à la clé en supposant a chaque fois si le nouveau bit est un 0 ou un 1, ensuite on calcule la corrélation entre la consommation réelle de l'énergie et les différents Hamming Weights pour trouver des fuites ; Alors, le plus grand coefficient de corrélation répond à la grande similitude entre la consommation et le poids calculé et donc représente si le bon bit est un 0 ou 1.

L'algorithme que j'ai utilisé dans mon programme est le suivant :

1. La récupération des traces + messages + modulo par l'initiation de la classe par le chemin qui correspond à mon dossier.
2. Calculer la clé privée à partir des messages cryptés et de leurs traces :
    a. On suppose que le premier bit fort est un 1.
    b. On fait une itération bit par bit pour estimer la valeur de chaque bit :
        i. Pour chaque bit, on calcule la corrélation entre les Traces à partir des données des courbes et les Hamming Weights de l'exponentiation modulaire du message et l'hypothèse de la clé pour 0.
        ii. Pour chaque bit, on calcule la corrélation entre les Traces à partir des données des courbes et les Hamming Weights de l'exponentiation modulaire du message et l'hypothèse de la clé pour 1.
        iii. Pour chaque bit, on compare les deux coefficients de corrélation et si :
            - La corrélation de 1 est la plus grande, on rajoute un bit de 1 avec la clé, et on passe deux mesures dans les traces (c'est justifié, car si le bit est 1, on peut clairement voir que dans l'algorithme « Baby RSA » on exécute 2 instructions et une seule pour un bit 0).
            - La corrélation de 0 est la plus grande, on rajoute un bit de 0 avec la clé, et on passe une mesure dans les traces.
    c. On inverse la clé résultante.