Rapport de restitution de TP de sécurité matérielle appliquée aux algorithmes PK

L’objectif de ce TP est d’effectuer une attaque par canaux cachés CPA sur l’algorithme de chiffrement RSA, en étudiant sa consommation électrique.

Nous avions le dossier de données numéro **donner numéro**

Réflexions

L’attaque CPA nécessite de déterminer les bits de la clé de chiffrement 1 à 1 en utilisant le résultat trouvé à l’indice précédent. On commence donc par une hypothèse sur le premier bit de la clé, par exemple en supposant qu’il vaut 1.

En observant l’algorithme de l’exponentiation modulaire, on remarque que si le ième bit de la clé privée d vaut 1, alors deux opérations sont effectuées, et une seule sinon. Il faut donc prendre cela en compte lors de l’attaque, car, ainsi, on sait quelle consommation de traces étudier.

Procédé

Afin d’attaquer le chiffrement RSA, nous avons procédé de la manière suivante :