Cartes à puce

Sécurité des Implémentations

Examen TP

Février 2018

Préambule

L'accès aux espaces "Cartes à puce : Sécurité des Implémentations" et "Développement Logiciel Cryptographique" de Community est autorisé. L'accès au web et au mail est interdit.

Vous rendrez votre travail (codes sources et fichiers générés par vos programmes) sous le forme d'un seul fichier archive que vous téléverserez sur l'espace de rendu sur Community.

Durée de l'examen : 2 heures.

Cet examen TP, à réaliser en langage C, est adossé au dernier TD réalisé, appelé "Pic de DPA", disponible sur Community.

On s'intéressera uniquement à la consommation de courant à l'instant de lecture en mémoire de la sortie d'une S-box au premier tour d'un AES. Vous considérerez que cette consommation de courant suit parfaitement le modèle dit "en poids de Hamming". Plus précisément, et afin de pouvoir donner des résultats "en unité bit", vous assimilerez tout simplement la consommation au poids de Hamming de la donnée manipulée, en ignorant tout bruit de mesure.

1 Hauteur du pic de DPA

Dans toute cette section vous utiliserez une valeur d'octet de clé égale à $k = 110$. Vous supposerez également que dans le processus d'attaque toutes les valeurs de l'octet de message m sont représentées une fois et une seule (DPA à 256 messages).

1.1 DPA classique

En référence aux deux premières questions de l'exercice 1 du TD, écrivez un programme qui sépare les messages en deux paquets selon la valeur du bit de poids fort de la sortie de S-box.

Votre programme devra générer deux fichiers texte différents correspondant aux deux paquets de "traces". Chaque fichier devra contenir la liste des messages dont les traces sont intégrées à ce paquet, ainsi que les consommations en sortie de S-box associées. Chaque ligne sera de la forme : *valeur de message : consommation*.

Votre programme devra également afficher à l'écran d'une part la consommation moyenne dans chaque paquet, d'autre part la hauteur du pic de DPA.

1.2 Variantes de DPA

Écrivez trois nouveaux programmes qui réalisent la même chose que celui de l'exercice précédent, mais cette fois-ci en considérant les trois variantes de DPA suivantes :

a) La variante à deux bits décrite à l'exercice 2 du TD. Pour le partitionnement des messages, vous utiliserez les deux bits de poids fort de la sortie de S-box, et non les deux bits de poids faible comme dans l'exercice.

b) La variante selon le poids de Hamming "fort ou faible" décrite en première partie de l'exercice 3 du TD.

c) La variante selon le poids de Hamming "très fort ou très faible" décrite en seconde partie de l'exercice 3 du TD.

2 Pics de DPA fantômes

L'exercice 4 du TD analyse de manière précise ce qu'il se passe lorsque l'hypothèse de clé est incorrecte (l'attaquant fait une hypothèse g différente de la vraie valeur k). Il y est suggéré que dans le cas d'une hypothèse de clé incorrecte il est faux de considérer que les consommations moyennes des deux paquets sont identiques.

2.1 Calcul du pic de DPA pour une hypothèse de clé incorrecte

En conservant la valeur $k = 110$, adoptez comme hypothèse de clé la valeur $g = 231$.

Écrivez un programme qui sépare les messages en deux paquets, en utilisant la variante de DPA selon le poids de Hamming "très fort ou très faible" (variante c) de l'exercice précédent).

Votre programme générera des fichiers similaires à ceux de vos programmes précédents, mais en considérant la valeur supposée de la clé pour ce qui est d'intégrer chaque message à l'un ou l'autre des paquets (ou aucun), et en considérant la valeur correcte de la clé pour ce qui est du calcul de la consommation.

Comme pour les autres exercices, votre programme devra afficher la consommation moyenne dans chaque paquet, ainsi que la hauteur du (faux) pic de DPA.

2.2 Calcul de l'ensemble des faux pics de DPA

L'avant-dernière question de l'exercice 4 du TD suggère que la hauteur d'un faux pic de DPA, qui semble a priori dépendre de k et de g, n'est en réalité qu'une fonction de $\delta = k \oplus g$.

Écrivez un programme qui affiche à l'écran pour l'ensemble de toutes les valeurs possibles de δ la hauteur du faux pic de DPA correspondant.