Examen de Cartes à Puce 2

Février 2016

Durée : 1h30

Les supports de cours de l'UE Cartes à Puce 2
sont les seuls documents autorisés pour la composition de cet examen.

L'usage d'une calculatrice est autorisé.

Exercice 1 (2,5 points)

On suppose un modèle de consommation linéaire en la distance de Hamming entre la donnée étudiée et un état de référence RF.

- Quelle relation existe-t-il entre le coefficient de corrélation calculé sur une série de consommations en supposant la valeur RF=5, et celui calculé sur la même série de consommations en supposant la valeur RF=250 ?

- En déduire une manière d'accélérer l'attaque par CPA en réduisant le nombre d'hypothèses à faire sur RF.

Exercice 2 (1 point)

- Est-il possible de retrouver de l'information sur la clé d'un DES ou d'un AES en exploitant par DPA ou CPA les traces de consommation relatives à l'exécution du key schedule ? Justifiez votre réponse.

Exercice 3 (2 points)

Une chaîne d'additions pour un entier a est une séquence d'entiers $a_1, a_2, \ldots, a_k$, ayant les propriétés suivantes : $a_1=1$, $a_k=a$, et pour tout $1 < j \leq k$, il existe deux indices $1 \leq i_1, i_2 < j$ tels que $a_j = a_{i1} + a_{i2}$. Calculer m^d mod n se fait en calculant des puissances de m successives dont les exposants forment une chaîne d'additions pour d.

- Pour d=109, quels sont les $d_j = d_{i1} + d_{i2}$ successifs lors d'une exponentiation par la méthode *square and multiply* de droite à gauche ?, par la méthode *Joye ladder* ?

Exercice 4 (4 points)

Soit E une fonction de chiffrement par blocs (DES ou AES par exemple). Une contre-mesure vis-à-vis des attaques par analyse de fautes consiste à faire exécuter à la carte deux fois le même calcul – $C_1 = E(K,M)$, puis $C_2 = E(K,M)$ – et à ne retourner la valeur du chiffré à l'appelant que si $C_1 = C_2$ (un code d'erreur est retourné dans le cas contraire).

- Expliquez contre quel type d'attaquant cette contre-mesure est efficace.

- Voyez-vous une façon d'adapter l'analyse différentielle de fautes (DFA) sur le DES pour pouvoir retrouver la clé malgré cette contre-mesure ? Si oui, expliquez en détails comment devra s'y prendre l'attaquant pour retrouver la clé.

- Voyez-vous une façon d'adapter l'analyse de fautes par collisions (CFA) sur l'AES pour pouvoir retrouver la clé malgré cette contre-mesure ? Si oui, expliquez en détails comment devra s'y prendre l'attaquant pour retrouver la clé.

Exercice 5 (3 points)

- Comparez entre elles l'analyse de courant par corrélation et l'analyse de templates selon tous les critères qui vous semblent pertinents.

  Conseil : ne recopiez pas mot pour mot des phrases toutes faites tirées de votre cours. Cela évitera d'agacer votre correcteur.

Exercice 6 (4 points)

Lors d'une attaque par DPA ou CPA sur un calcul $s = m^d \bmod n$ de signature RSA[1] par un algorithme d'exponentiation à parcours de l'exposant de gauche à droite, on suppose que l'attaquant connaît déjà la valeur $t = (d_{k-1}, \ldots, d_{i+1})_2$, et il doit obtenir la valeur du bit suivant d_i.

Pour ce faire, une première méthode consiste à détecter la présence ou l'absence d'un pic sur la trace de DPA ou de CPA obtenue en considérant la valeur intermédiaire $v_1 = m^{2t+1} \bmod n$.

Une deuxième méthode consiste à détecter la présence ou l'absence d'un pic sur la trace de DPA ou de CPA obtenue en considérant la valeur intermédiaire $v_1 = (m^{2t+1})^2 \bmod n$.

Une troisième méthode consiste à comparer les traces de DPA ou de CPA obtenues en considérant les valeurs intermédiaires $v_0 = (m^{2t})^2 \bmod n$ et $v_1 = (m^{2t+1})^2 \bmod n$.

- Expliquez en quoi selon vous la deuxième méthode pourrait être avantageuse par rapport à la première.

- Expliquez en quoi selon vous la troisième méthode pourrait être avantageuse par rapport à la deuxième.

1 Pour la simplicité de l'écriture, on fait ici abstraction de l'utilisation de la fonction de hachage.

Exercice 7 (1,5 points)

- Lorsqu'on calcule une trace de DPA pour la bonne hypothèse de clé, il arrive que le pic de DPA obtenu soit négatif. Quelle explication pouvez-vous donner à ce phénomène ?

Exercice 8 (2 points)

- Est-il plus intéressant d'utiliser une représentation signée de l'exposant/scalaire dans le cas d'une exponentiation modulaire RSA, ou dans le cas d'une multiplication scalaire sur courbe elliptique ?

- Dans celui des deux cas qui vous paraît le plus adapté à la représentation signée, quel avantage tire-t-on de cette représentation par rapport à la représentation classique ?