Examen de Cartes à Puce 2

Septembre 2017

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 (4,5 points)

On suppose le modèle de consommation linéaire en le poids de Hamming suivant :

$$conso(x) = a \cdot HW(x) + b$$

- Dans un attaque par DPA sur l'AES, que représente le "x" du modèle ci-dessus ?

- On suppose que les coefficients *a* et *b* valent respectivement a = 2,5 et b = 158. Quelle est la valeur de la consommation lorsque *x* vaut 63 ? Et lorsque *x* vaut 66 ?

- Si on fait une DPA, on met dans le paquet "1" les traces pour lesquelles le bit de poids fort de *x* vaut 1, et dans le paquet "0" celles pour lesquelles ce bit vaut 0.
  En supposant une distribution uniforme de *x*, quelle sera la valeur théorique du pic de DPA, c'est à dire la différence de consommation moyenne lors de la manipulation de *x* entre le paquet "1" et le paquet "0" ?

Exercice 2 (5 points)

- Expliquez en quoi consiste le masquage d'exposant appliqué à une exponentiation modulaire. De quels types d'attaques cette contre-mesure est-elle sensée protéger ?

- Expliquez pourquoi le masquage d'exposant est inutile si l'attaquant est capable de retrouver l'exposant utilisé lors d'une exponentiation par SPA en n'utilisant qu'une seule trace.

Exercice 3 (3,5 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 4 (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.

Exercice 5 (3 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 ?

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