Cartes à puce 2

Examen écrit (session 2)

Septembre 2016

Consignes

La durée de cette épreuve est de 1h30. Les supports de cours, de TD et de TP de CAP 2 sont les seuls documents que vous êtes autorisés à consulter. L'usage d'une calculatrice est autorisé.

1 Exponentiations modulaires

1. Lors du calcul de $s = m^d \bmod n$, décrivez en détail le fonctionnement pas à pas des différentes méthodes d'exponentiation suivantes (en précisant entre autre les valeurs intermédiaires prises par les différents registres) en supposant que la valeur de l'exposant est $d = 50$:
   — Montgomery Ladder
   — Square & Multiply binaire de gauche à droite
   — Square & Multiply Always binaire de droite à gauche

2. On suppose qu'un attaquant est capable de repérer sur une trace de courant d'un calcul de signature RSA la succession des opérations modulaires sur grands entiers, ainsi que le type – Square ou Multiply – de ces différentes opérations.

   (a) Est-ce qu'il lui est possible de casser la clé par analyse de la trace de courant pour les différentes méthodes d'exponentiation suivantes :
   — Square & Multiply binaire de droite à gauche
   — Joye Ladder
   Vous prendrez soin de justifier votre réponse.

   (b) Même question mais en considérant cette fois que la valeur de l'exposant est randomisée à chaque exécution. Précisez ce que l'on doit comprendre ici par "casser la clé".

3. Il est souvent considéré que la multiplication scalaire d'un point d'une courbe elliptique et l'exponentiation modulaire RSA sont deux formes différentes d'un même algorithme, et que les mêmes types d'attaques side-channel peuvent s'y appliquer. C'est à la fois vrai et faux...

   Expliquez en quoi la multiplication scalaire et l'exponentiation (ainsi que les attaques s'y appliquant) sont similaires, et en quoi elles sont différentes.

2 Autour de la DPA et de la CPA

1. On souhaite réaliser une analyse de courant par corrélation sur le DES.

   (a) Combien de traces de CPA doit-on générer pour attaquer la première S-Box du premier tour ? Quelle quantité d'information sur la clé cela permet-il de retrouver ?

   (b) Combien de traces de CPA doit-on générer au total pour attaquer toutes les S-Box du premier tour ? L'information secrète globale retrouvée permet-elle de connaître la valeur de la clé de chiffrement ?

   (c) En quoi les réponses aux questions 1a et 1b précédentes seraient différentes dans le cas d'une DPA plutôt que d'une CPA ?

2. Répondez aux mêmes questions que ci-dessus (1a, 1b et 1c) dans le cas où la fonction de chiffrement attaquée est l'AES.

3. Est-il possible de réaliser une DPA sur l'AES lorsque les entrées M_i de l'algorithme ne sont pas connues ? Expliquez.

3 Analyse de fautes

1. Est-il possible de réaliser une analyse différentielle de faute sur le DES lorsque les entrées de l'algorithme ne sont pas connues ? Expliquez.

2. Est-il possible de réaliser une analyse de fautes par collision sur l'AES lorsque les entrées de l'algorithme sont connues mais pas choisies par l'attaquant ? Expliquez.