Sécurité physique des cartes à puces

TP – Analyse de canaux auxiliaires (DPA, CPA)

Christophe Clavier

1 Préliminaires

L'objet de ce TP est de mettre en œuvre différentes attaques par analyse de canaux auxiliaires telles que l'analyse différentielle du courant (DPA) et l'analyse du courant par corrélation (CPA).

Les signaux traités sont des courbes capturées en cas réel et qui reflètent la variation de la consommation électrique mesurée aux bornes d'une puce cryptographique en fonctionnement. La commande exécutée calcule le résultat C d'un chiffrement AES, sous la clé secrète K, d'une entrée M connue de l'attaquant.

Les courbes utilisées dans ce TP ont été préalablement acquises. La portion de signal contenue dans ces $N = 2000$ courbes correspond aux calculs successifs des 16 opérations SBOX du dernier tour. Chaque courbe est composée de $T = 29000$ points.

Nommage des courbes Les fichiers de courbe sont nommés selon le format "%s_%04d" où le premier champ (préfixe commun à toutes les courbes) a pour valeur "demo", et où le deuxième champ (l'index de la courbe) varie entre 0 et $N - 1$. Par exemple a courbe n° 42 a pour chemin relatif curves/demo_0042. Par ailleurs, les fichiers "demo_input.txt" et "demo_output.txt" contiennent respectivement les messages et les chiffrés des N exécutions.

Question 1.1 *A l'aide d'un logiciel approprié (Gnuplot, Matlab, Maple, Mathematica,. . .), chargez une ou plusieurs courbes et visualisez les sur un même graphique.*

Question 1.2 *Écrire un programme qui calcule la courbe "moyenne" μ définie comme l'ensemble des moyennes des courbes $\mathcal{C}_i$ à chaque instant t :*

$$\forall\, t = 1, \ldots, T \qquad \mu[t] = \frac{1}{N} \sum_{i=0}^{N-1} \mathcal{C}_i[t]$$

Visualisez simultanément cette courbe moyenne avec quelques courbes brutes.

2 Analyse différentielle du courant

L'analyse différentielle du courant (DPA) consiste essentiellement en un test d'hypothèse portant sur une petite portion de la clé secrète K.

Dans le cas de l'AES, la valeur v d'une donnée intermédiaire manipulée par le micro-processeur pendant le calcul cryptographique ne dépend que d'un octet c du chiffré C et d'un octet k (appelée sous-clé) de la clé K_{10} du dernier tour. On a ainsi :

$$v = f(c, k)$$

Par exemple, v peut représenter l'entrée d'une SBOX du dernier tour d'AES. On a alors :

$$v = SBOX^{-1}(c \oplus k)$$

Pour chaque valeur supposée g de la sous-clé k et pour chaque exécution d'index i, il est possible de calculer une prédiction de la donnée intermédiaire :

$$v_i^{(g)} = f(c_i, g) = SBOX^{-1}(c_i \oplus g)$$

A fortiori et considérant la représentation binaire :

$$(v_{i,7}^{(g)}, v_{i,6}^{(g)}, v_{i,5}^{(g)}, v_{i,4}^{(g)}, v_{i,3}^{(g)}, v_{i,2}^{(g)}, v_{i,1}^{(g)}, v_{i,0}^{(g)})$$

de $v_i^{(g)}$, il est possible de prédire l'un quelconque de ces bits :

$$v_{i,b}^{(g)} = f_b(c_i, g)$$

Dans l'analyse différentielle du courant, pour chaque supposition g sur la sous-clé on réalise une partition de l'ensemble des courbes en deux parties selon la valeur supposée du bit b :

$$\mathcal{S}_0^{(g)} = \left\{ \mathcal{C}_i : v_{i,b}^{(g)} = 0 \right\}$$

$$\mathcal{S}_1^{(g)} = \left\{ \mathcal{C}_i : v_{i,b}^{(g)} = 1 \right\}$$

Si g est la valeur correcte k de la sous-clé alors la partition est cohérente avec la valeur du bit b réellement manipulée par la puce. On s'attend dans ce cas à ce que la consommation de courant à chaque instant où ce bit est manipulé soit en moyenne plus élevée dans le paquet $\mathcal{S}_1^{(g)}$ que dans le paquet $\mathcal{S}_0^{(g)}$ (si toutefois le modèle de consommation prévoit qu'un bit à 1 "consomme" plus qu'un bit à 0). Cette différentielle sera mise en évidence en calculant les différentes courbes de DPA définies comme différences des courbes moyennes de chaque paquet :

$$\Delta^{(g)} = \left\langle \mathcal{S}_1^{(g)} \right\rangle - \left\langle \mathcal{S}_0^{(g)} \right\rangle$$

Pour $g = k$, la courbe de DPA doit présenter une valeur significativement supérieure à 0 en valeur absolue (pic de DPA) lorsque le bit b est manipulé. En revanche, si g est une supposition incorrecte de la sous-clé, alors le partitionnement est supposé être incohérent avec la valeur réelle du bit b et la courbe de DPA sera uniformément proche de 0 (pas de pic).

Question 2.1 *Écrivez un programme qui prend en entrée :*
- *le numéro d'un octet de clef à retrouver*
- *le numéro du bit choisi pour le partitionnement des courbes*

et qui calcule les courbes de DPA ($\Delta^{(g)}$) associées à chaque valeur supposée g de la sous-clé ciblée. Votre programme déterminera la hauteur du plus haut pic (en valeur absolue) sur chaque courbe de DPA et en déduira la valeur présumée de k.

Question 2.2 *Utilisez votre programme de DPA pour retrouver les valeurs des 16 octets de la clef du dernier tour.*

Question 2.3 *Décrire le mode opératoire qui permettrait à l'attaquant de retrouver la clé s'il dispose des messages mais pas des chiffrés.*

3 Analyse du courant par corrélation

L'analyse du courant par corrélation (CPA) est une évolution de la DPA présentant deux différences essentielles avec celle-ci :
- on considère la valeur de l'intégralité du mot machine contenant la donnée intermédiaire plutôt que celle d'un bit seulement,
- on utilise un modèle de consommation (correct à une transformation linéaire près) pour corréler les consommations mesurées et leurs prédictions issues du modèle.

Supposons un modèle de consommation dépendant linéairement du poids de Hamming (HW) de la donnée manipulée :

$$w = \alpha \cdot HW(v) + \beta \qquad (\alpha \text{ et } \beta \text{ constantes inconnues})$$

Dans le cas $g = k$, la série des poids de Hamming des $v_i^{(g)}$ est alors fortement (linéairement) corrélée à la série des consommations mesurées à l'instant (ou aux instants) où la donnée intermédiaire est manipulée.

Dans le cas $g \neq k$, il y a décorrélation entre les séries de poids de Hamming et de consommations mesurées.

Question 3.1 *Réaliser un programme qui utilise le coefficient de corrélation linéaire (plutôt que le partitionnement et la différence des moyennes) pour calculer les courbes de CPA sous chaque hypothèse de sous-clé.*

Question 3.2 *Utiliser le programme de CPA pour retrouver les valeurs des sous-clés du dernier tour.*

Modifiez le programme d'attaque par CPA pour qu'il fonctionne sous le modèle plus général d'une consommation dépendant linéairement de la distance de Hamming (HD) entre la valeur prédite et un état de référence constant ref :

$$w = \alpha \cdot HD(v, ref) + \beta = \alpha \cdot HW(v \oplus ref) + \beta$$

Question 3.3 *Quelle valeur de référence ref_{max} donne les plus grands pics de CPA ?*

Question 3.4 *Pour l'octet de K_{10} de votre choix, et connaissant maintenant la valeur de cet octet, calculez les courbes de DPA pour chacun des 8 bits cibles. Pour chacune de ces courbes relevez le signe du pic et trouvez un lien entre ces différents signes et la valeur ref_{max}.*