Examen – Attaques sur carte à puce 2016-2017

Durée : 1h

Alberto Battistello

a.battistello@oberthur.com

Exercice 1. Attaques Physiques.

L'implémentation des cryptosystems modernes demande une grande attention pour les protéger des attaques. Nous avons vu en cours que les données sensibles manipulées par les algorithmes comme AES, DES, RSA etc... peuvent être récupérer à partir d'attaques physiques sur les systèmes sur lesquelles ces algorithmes cryptographiques sont exécutées.

1. Expliquer la différence entre une attaque de cryptanalyse classique et une attaque physique. `[0.25 pt]`
2. Donner quelques exemple de model de faute utilisées dans les attaques par faute. `[0.25 pt]`
3. Nous avons vu en cours la DFA sur l'algorithme DES avec une faute sur l'entrée du dernier round (cf. Figure 1). Détailler le procédé qui permet de distinguer une bonne hypothèse de clef d'une mauvaise hypothèse de clef. `[1 pt]`

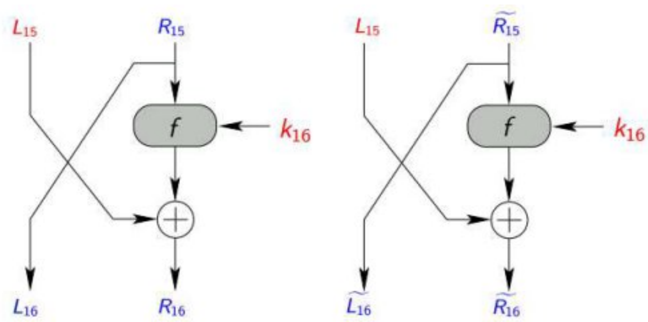

FIGURE 1 – DES avec et sans faute sur l'entrée du dernier round.

Exercice 2. Algorithme RSA.

Algorithm 1: Montgomery Ladder

Input : Le message m, l'exposant privé $d = (d_{n-1}, \ldots, d_0)_2$ et le modulus N

Output: La signature $S = m^d \bmod N$

$R_0 \leftarrow 1$;
$R_1 \leftarrow m$;
for $i \leftarrow n-1$ **to** 0 **do**
  if $d_i == 0$ **then**
    $R_1 \leftarrow R_0 R_1 \bmod N$; $R_0 \leftarrow (R_0)^2 \bmod N$;
  if $d_i == 1$ **then**
    $R_0 \leftarrow R_0 R_1 \bmod N$; $R_1 \leftarrow (R_1)^2 \bmod N$;
return R_0;

Algorithm 2: Square-and-Multiply Always

Input : Le message m, l'exposant privé $d = (d_{n-1}, \ldots, d_0)_2$ et le modulus N

Output: La signature $S = m^d \bmod N$

$R_0 \leftarrow 1$;
for $i \leftarrow n-1$ **to** 0 **do**
  $R_0 \leftarrow R_0^2 \bmod N$;
  $R_1 \leftarrow R_0 \cdot m \bmod N$;
  $R_0 \leftarrow R_{d_i}$;
return R_0;

1. Expliquer pourquoi utiliser l'algorithme *Square-and-Multiply Always* (cf. Alg. 2) pour calculer une signature RSA peut avantager un attaquant qui peut injecter des fautes perturbant le calcul d'une multiplication. Est-ce-que l'algorithme *Montgomery Ladder* (cf. Alg. 1) a le même type de problème ? `[1 pt]`

   Nous avons vu en cours le cryptosystème CRT-RSA. Ce système permets d'améliorer les performances de l'algorithme RSA classique en utilisant les propriétés du théorème des restes chinois.

2. Rappeler le gain moyen en performances du CRT-RSA par rapport à un RSA classique et l'expliquer. `[1 pt]`
3. L'attaque "BELLCORE" que on a étudié en cours permet de retrouver l'un des facteur premier (p ou q) du module n du RSA à partir des paramètres publiques (n, e), d'une signature valide S et d'une signature fauté $\tilde{S}$. Suggérer une adaptation de l'attaque dans le cas où l'attaquant ne connais pas la valeur de la signature correct S mais il connais le message m qui a été signé, ainsi que les paramètres publiques (n, e), et la signature fauté $\tilde{S}$. `[1 pt]`

Exercice 3. Analyse side-channel et recombinaison CRT-RSA.

Pour récombiner les deux sous-exponentiations modulaires (S_p, S_q) d'un CRT-RSA, un'implémentation utilise la recombinaison de Garner, qui consiste á calculer la signature S comme :

$$S = Sq + q \cdot (i_q(S_p - S_q) \bmod p) \ ,$$

oú $i_q = q^{-1} \bmod p$.

Un attaquant observe que :

$$\left\lfloor \frac{S}{q} \right\rfloor = i_q(S_p - S_q) \bmod p + \left\lfloor \frac{S_q}{q} \right\rfloor \ .$$

Étant S_q toujours plus petit que q, cela implique que $\left\lfloor \frac{S_q}{q} \right\rfloor = 0$. L'attaquant obtient donc l'équation suivante :

$$\left\lfloor \frac{S}{q} \right\rfloor = i_q(S_p - S_q) \bmod p \ .$$

Étant donné que la valeur $i_q(S_p - S_q) \bmod p$ est manipulée pendant le calcul, et que S est connu par l'attaquant, expliquer comment l'attaquant peut exploiter cela avec une attaque par side-channel différentielle pour retrouver la valeur sensible q.`[1.5 pt]`