Analyse de la consommation instantannée de courant sur RSA

Kévin Boyeldieu
Titouan Tanguy
TLS-SEC

Mars 2018

Abstract

Le but de ce challenge est de montrer comment l'analyse de la consommation instantannée de courant d'un cryptosystème cryptographiquement sûr peut le compromettre si son implémentation n'est pas rigoureuse. Nous vous proposons de réaliser à travers une simulation web chaque étape de l'attaque (de la préparation du circuit électronique à l'analyse sur l'oscilloscope) afin de casser l'algorithme RSA implémenté sur un Arduino Nano. Parviendrez vous à retrouver la clé privée?

Description du tutoriel

L'objectif de ce tutoriel est de réaliser chacune des étapes d'une attaque par consommation instannée de courant afin de prendre conscience des dangers d'une implémentation non rigoureuse d'un algorithme mathématiquement sûr. Ces différentes étapes sont les suivantes :

1- réfléchir à un moyen de mesurer la consommation instannée de courant du circuit;

2,3- préparer le circuit en y soudant et dessoudant certains composants;

4- analyser les résultats obtenus sur l'oscilloscope pour casser l'algorithme implémenté sur la carte.

Nous vous proposons dans ce tutoriel de casser l'algorithme RSA, implémenté sur une carte Arduino Nano. Les spécifications de cette carte sont fournies dans le fichier *arduino_nano_specs.png*. La documentation du micro contrôleur utilisé par l'Arduino Nano est également jointe, dans le pdf *ATmega328:P.pdf*. Pour vous faciliter la tâche, chaque étape devra être correcte et validée afin de passer à la suivante. Le tutoriel se termine lorsque vous parvenez à retrouver la clé privée utilisée par le cryptosystème.

Pour comprendre comment exploiter les résultats lors de la dernière étape de l'attaque, voici le code contenu dans la carte:

```
c : message chiffre
m : message dechiffre
d : cle privee
n : modulo

while true:
    // RSA : calcul de c^d mod n
    r = 1
    pour chaque bit de d:
        r = r*r mod n
        if bit == 1:
            r = r*c mod n
    m = r
```

En outre, on admettra que le calcul d'une multiplication modulaire nécessite environ 100 cycles d'horloges.