Programmation cartes à puces

Loïc Demange
loic.demange@etud.univ-paris8.fr

avec les notes de cours de Philippe Guillot

28/8 avril 2021

Attaques de consommation

En cryptanalyse, l'attaque de consommation consiste à analyser les traces de consommation d'un dispositif pour en déduire des informations sur le secret.

De manière générale, on consomme davantage lorsqu'un bit change d'état (de 0 à 1 ou inversement).

Attaques de consommation

Exemple sur le Square and Multiply.

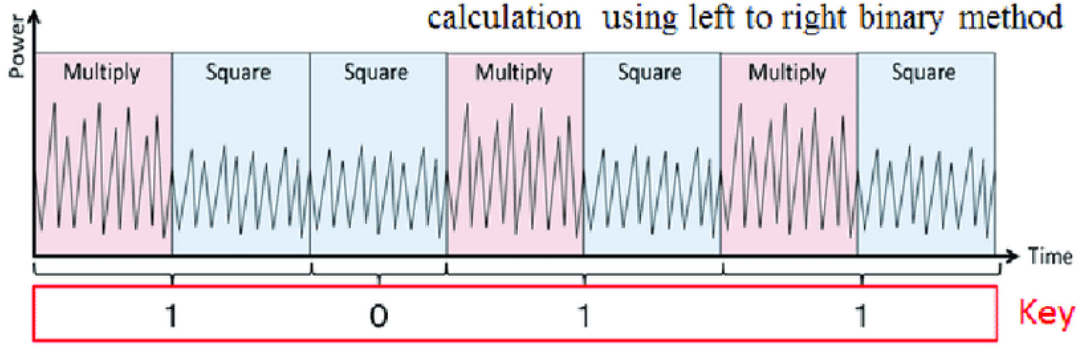
$$C = P^e \bmod N$$
$$P = C^d \bmod N$$

C: Cipher Text
P: Plain Text
e: Public Key
d: Private Key
N: modulo

(a) RSA crypto algorithm

```
input : X, N, d = (d_{k-1}, d_{k-2}, ....., d_0)
output: Z = X^d mod N
Z←1;
For i = k − 1 down to 0 do
  Z ←Z×Z mod N;     //Square
    if (d_i = 1) then
    Z←Z×X mod N;  //Multiply
  end
end
return Z;
```

(b) Modular exponentiation (X^d mod N) calculation using left to right binary method



(c) Power dissipation model during modular exponentiation

Figure: Tamper-resistant cryptographic hardware (Takeshi Fujino, Takaya Kubota, Mitsuru Shiozaki)

Attaques de consommation

Dans le projet carte SIM, le code PIN et le code PUK sont des secrets.

- Comment la vérification du code PIN/PUK peut faire fuiter de l'information ?

Attaques de consommation

On ne peut pas empêcher une action de consommer de l'énergie.
Le but est donc de décorreler la consommation du secret.

Projet carte SIM

Adapter la comparaison des codes PIN et PUK pour qu'elle ne fuite plus d'informations.