Dis moi ce que tu consommes, je te dirai qui tu es.

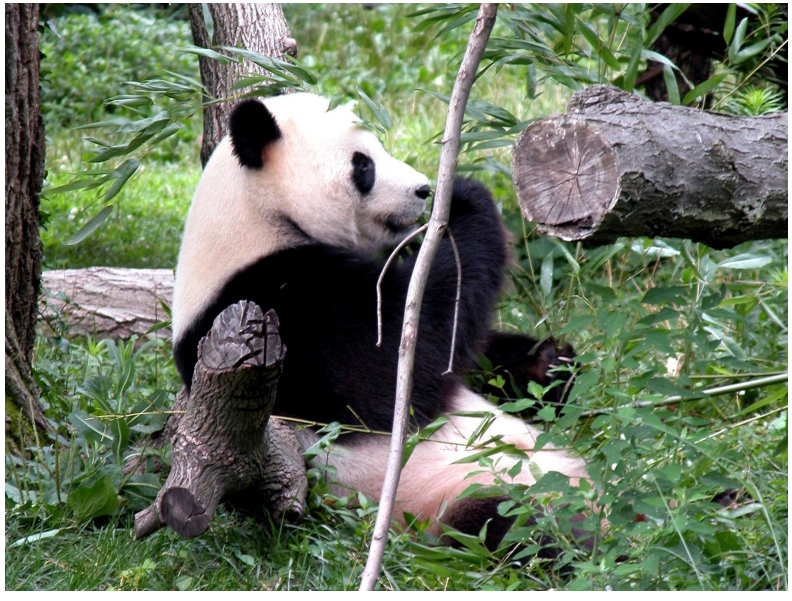
Nadia EL MRABET
J. C. Bajard & S. Duquesne

LIRMM - I3M - CNRS - Université Montpellier II

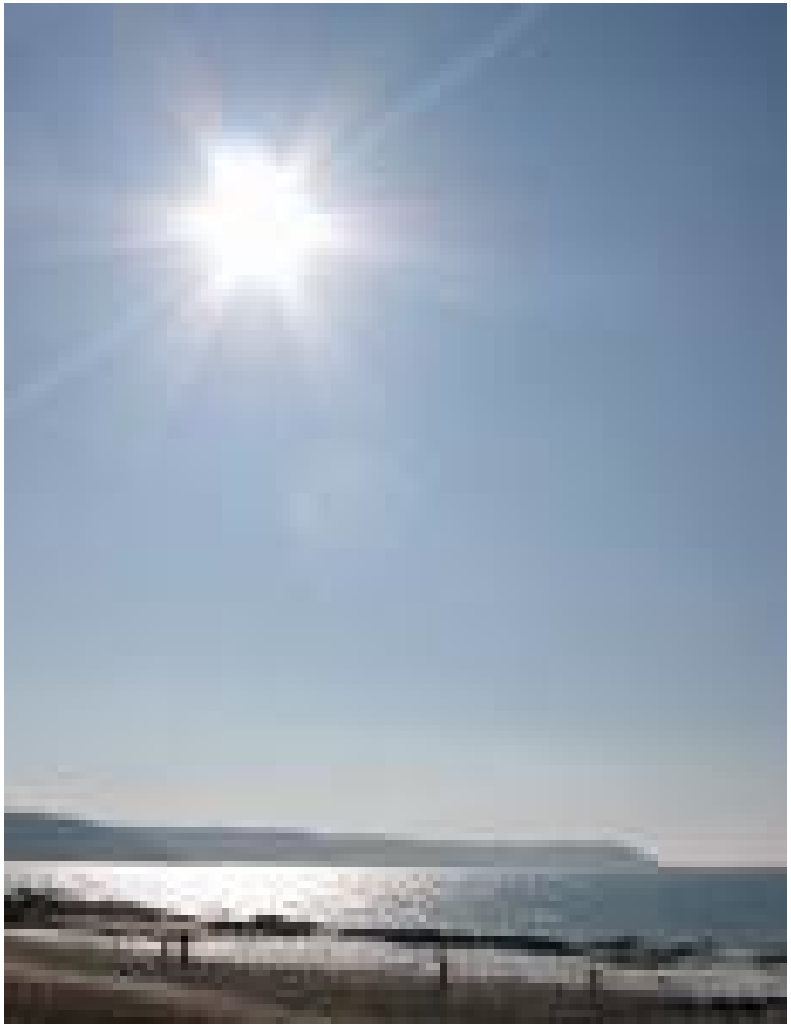
Doctiss08
10 avril 2008

Bambou

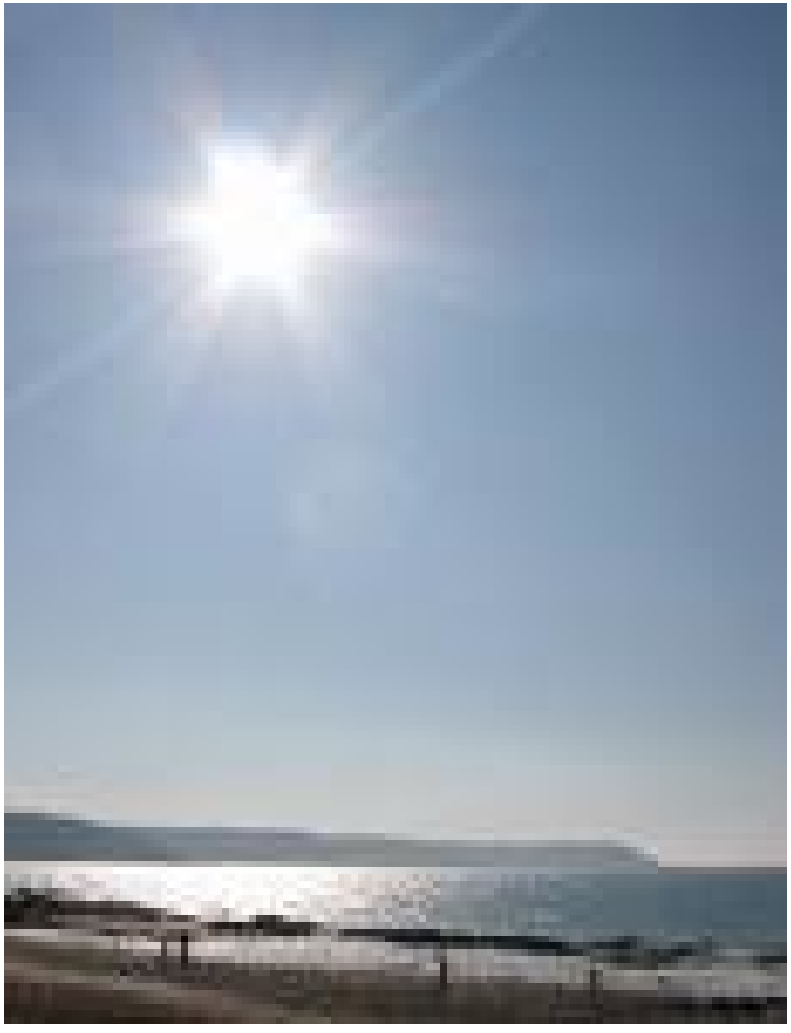
Bambou



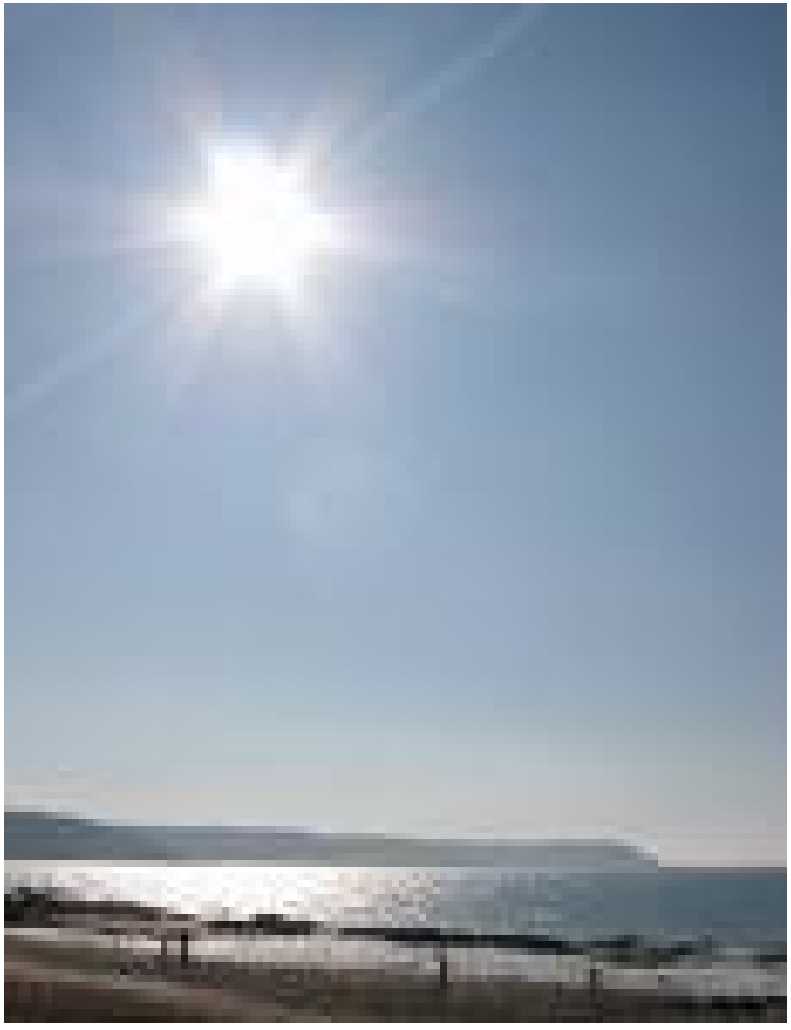
Energie solaire

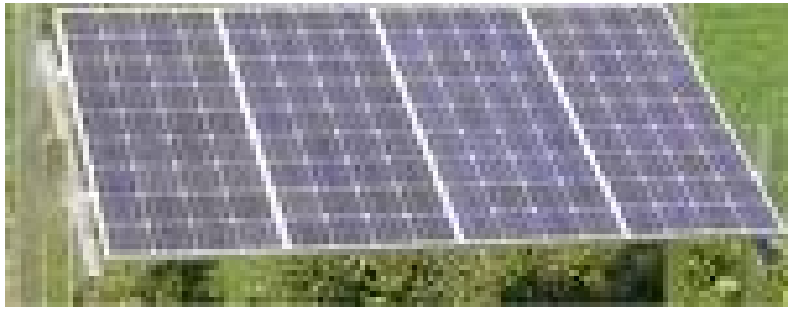


Energie solaire

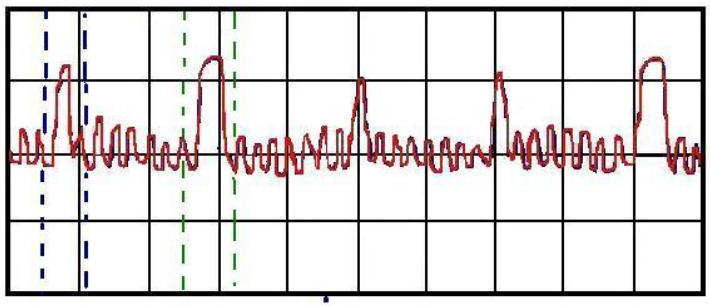


Energie solaire

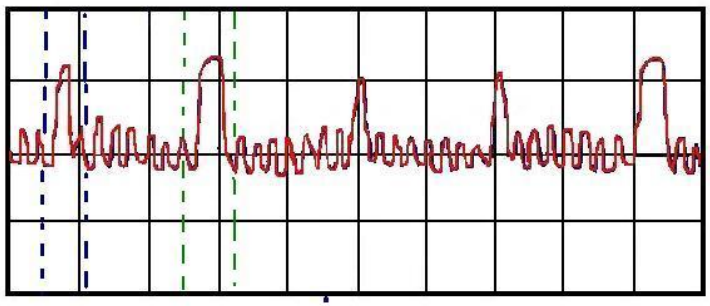


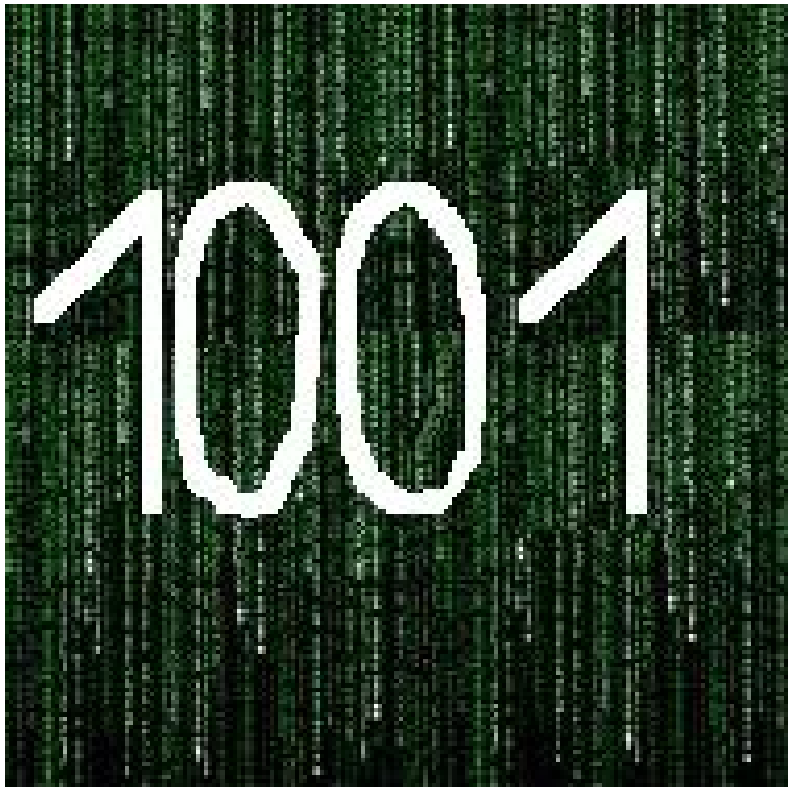


Electricité



Electricité





Plan

1. Introduction à la cryptographie
2. Exemple de protocle cryptographique : RSA
3. Attaque SPA
4. Contre mesures à l'attaque décrite
5. Conclusion

Cryptographie

Définition

"Ensemble des principes, méthodes et techniques dont l'application assure le chiffrement et le déchiffrement des données afin d'en préserver la confidentialité et l'authenticité".

Autrement dit, tout moyen permettant de communiquer avec quelqu'un sans que des personnes étrangères (i.e. des espions) ne puissent récupérer et surtout comprendre les messages.

Cryptographie

Exemple de protocole cryptographique

Exemple

- Nabuchodonosor, roi de Babylone
  - $\Rightarrow$ Raser ses esclaves et se servir de leur crane comme papyrus
- César, empereur romain
  - $\Rightarrow$ Chiffrement de César : décalage des lettres de l'alphabet
- Enigma, machine de communication allemande pendant la seconde guerre mondiale
  - $\Rightarrow$ Héritière du chiffrement de César

Point commun & inconvénient

La méthode de chiffrement est elle même secrète.

Principe de Kerckhoffs

La sécurité d'un protocole cryptographique doit être garantie par les clés de chiffrement et déchiffrement utilisées, et non par la méthode de chiffrement.

Conséquences

$\Rightarrow$ Naissance de la cryptographie moderne

- Caractérisation :
  - la méthode de chiffrement est connue de tous
  - la méthode de déchiffrement nécessite une clé secrète
- Le couple (clé publique, clé secrète) est construit de manière à ce que pour un protocole donné il soit difficile de retrouver la clé secrète à partir de la clé publique.

RSA

Découverte & Utilisation

Le protocole RSA du nom de ses inventeurs Rivest Shamir Adleman est un protocolé assymétrique à clé publique.
Il est utilisé à tous les niveaux de la société.

- Au gouvernement et bien sur par les armées
- le système bancaire
- carte à puce
- sur internet pour le commerce et l'échange de données
- pour le téléphone mobile
- la télévision payante...

RSA

Principe

La sureté du protocole RSA réside dans la difficulté à factoriser des grands nombres.

- La clé publique est un couple d'entier (N, e)
  - $\Rightarrow$ $N = pq$ avec p, q deux nombres premiers
  - $\Rightarrow$ $\phi(N) = (p-1) \times (q-1)$
  - $\Rightarrow$ $e \in [0; \phi(N)]$
- La clé privée est un entier d tel que
  - $\Rightarrow$ $ed \equiv 1 \bmod(\phi(n))$

RSA

Chiffrement - Déchiffrement

On considère qu'un message M est un chiffre.

- Méthode de chiffrement : $C = M^e \mod(N)$
- Méthode de déchiffrement : $M = C^d \mod(N)$

Théorème

- $N = pq$
- $(e, d) \in [0; \phi(N)]^2$ vérifiant $e \times d \equiv 1 \mod(\phi(N))$
- $M \in [0; N-1]$
- on sait que $M^{ed} \equiv M \mod(N)$.

RSA

Cryptanalyse

Cryptanalyse

But d'un espion : retrouver l'exposant secret d.

Méthode

- Recherche exhaustive $\Rightarrow$ bien trop long
- Récupérer d directement chez l'utilisateur $\Rightarrow$ bien trop voyant
- Ruser $\Rightarrow$ bien plus malin
- Attaques à canaux cachées.

Attaque à canaux cachées

Attaque permettant de retrouver le secret utilisé en relevant le temps d'exécution, la consommation électrique...

SPA

Description

Faille de RSA : l'exponentiation

La méthode la plus simple pour faire l'exponentation d'un entier par un autre est la méthode d'exponentiation rapide.
Sa consommation électrique est directement liée à l'exposant.

Simple Power Analysis

Cette méthode consiste à retrouver des informations par l'analyse de la courbe représentative de la consommation de courant lors de l'exponentiation à la puissance d.
Cette courbe de consommation est différente suivant les instructions exécutées et les données manipulées.

SPA

Algorithme d'exponentiation rapide

Algorithme d'exponentiation rapide

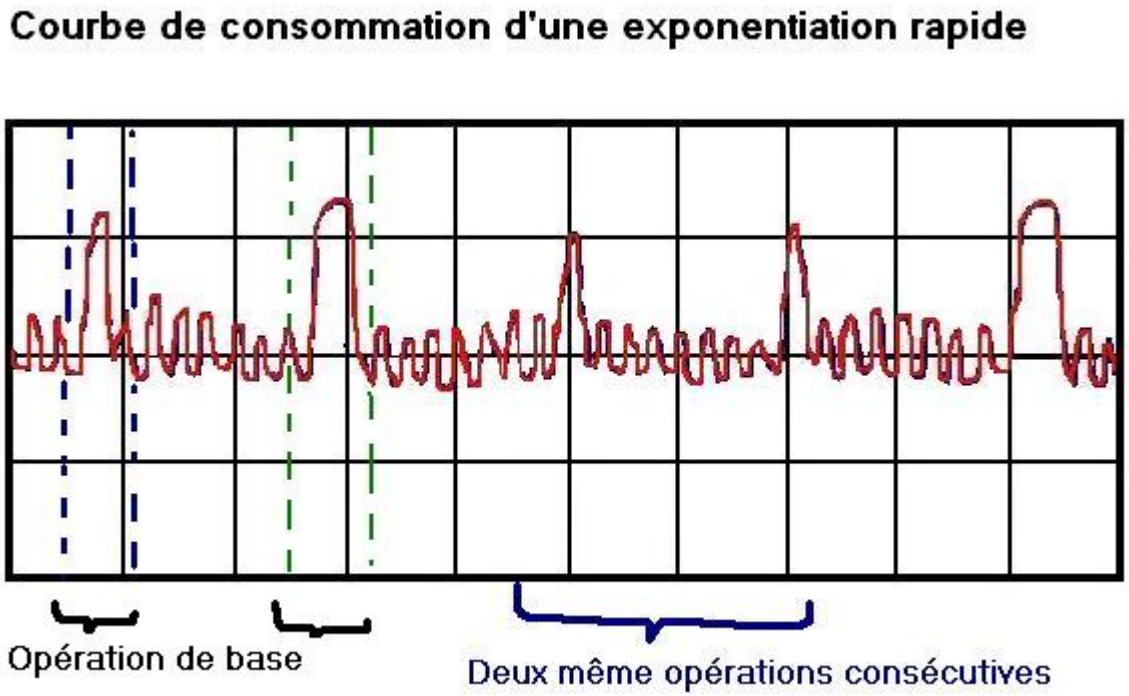
On veut calculer C^d

1 - Calculer la décomposition binaire de d, $d = \overline{d_n d_{n-1} \dots d_1 d_0}^2$
2 - $T \leftarrow C$
3 - **Pour** $i = n - 1$ **à** 0 **faire**
4 - $\quad T \leftarrow T \times T$
5 - $\quad\quad$ **Si** $d_i = 1$ **Alors** $T \leftarrow T \times C$
6 - **Renvoyer** T

SPA

Courbe de consommation de l'exponentiation rapide

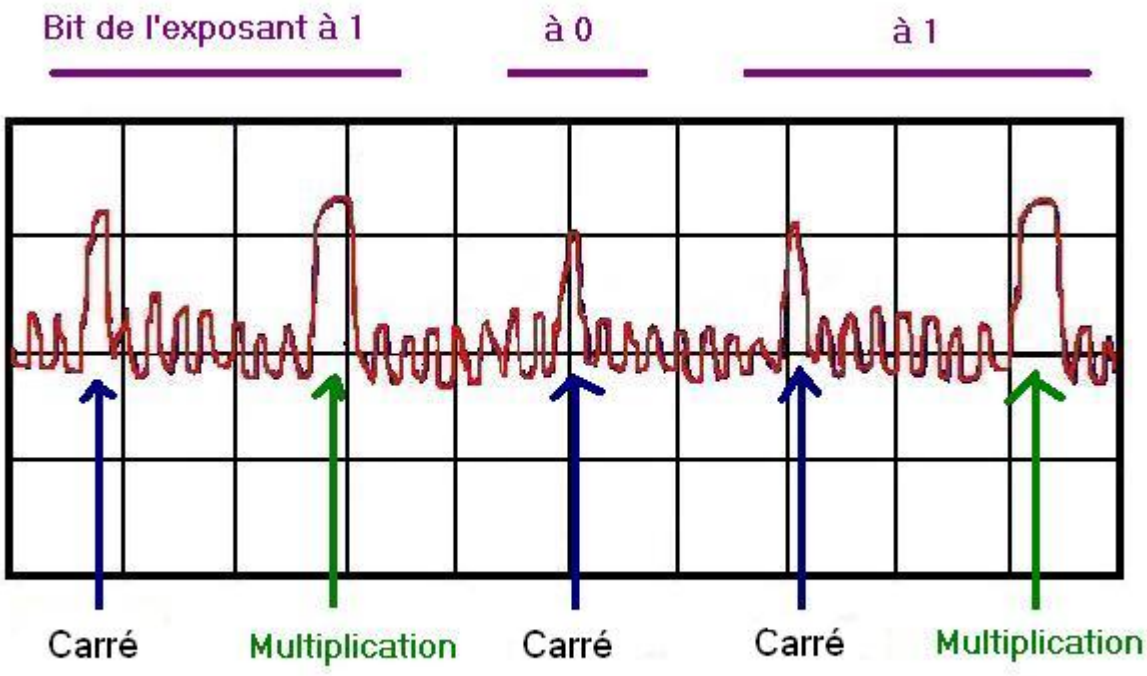
Courbe de consommation



SPA

Courbe de consommation de l'exponentiation rapide

Analyse de la courbe



SPA

Contre mesure

Consommation constante

Pour ne plus pouvoir découvrir l'exposant en lisant la courbe de consommation il faut qu'elle soit constante.

Pour ce faire : on utilise des opérations factices.

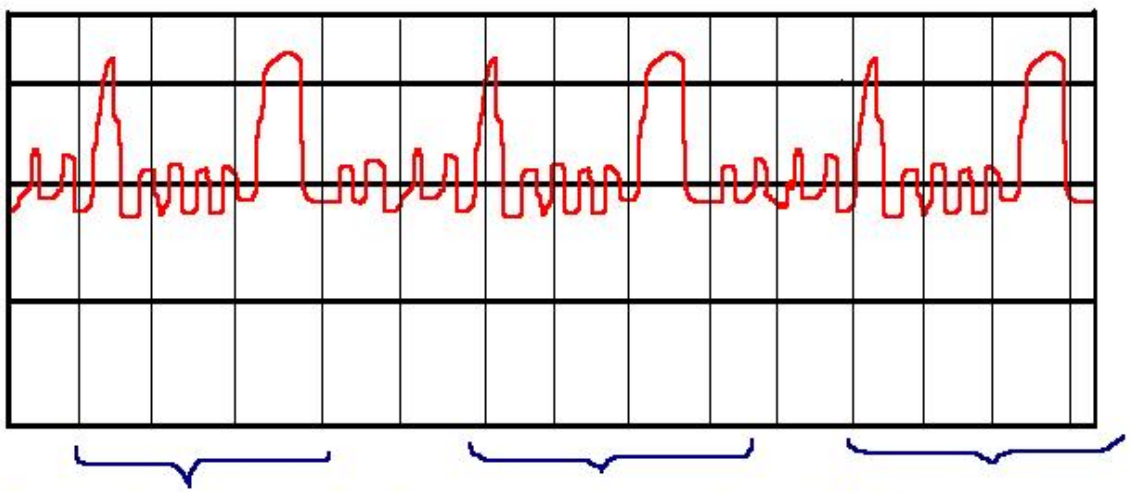
Modification pour consommation constante

1 - $T \leftarrow C$ et $U \leftarrow T$
2 - **Pour** $i = n - 1$ **à** 0 **faire**
3 - **Si** $d_i = O$ **Alors** $T \leftarrow T \times T$ et $U \leftarrow T \times C$
4 - **Si** $d_i = 1$ **Alors** $T \leftarrow T \times T$ et $T \leftarrow T \times C$

SPA

Contre mesure

Courbe de consommation de l'algorithme transformé



Toujours la même courbe de consommation quelque soit le bit en cours

Conclusion

L'utilisation des fuites d'informations permet de retrouver des informations sur le secret utilisé.
L'ajout d'opérations factices empêche de lire directement la clé.
Pour retrouver malgré tout des informations :
Essayer de déterminer quelles sont les opérations factices, ce qui peut se faire en provoquant des erreurs.

"C'est en faisant des erreurs qu'on apprend."

Merci pour votre attention.
Des questions ?