

Opérateurs arithmétiques sécurisés

Arnaud Tisserand

CNRS, IRISA, Équipe-projet CAIRN

RAIM

Lyon, 26-28 octobre 2009



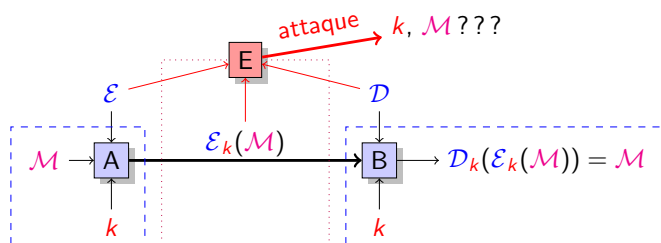
Les besoins en **dispositifs de cryptographie** sont de plus en plus grands :

- pour faire du **chiffrement** (ssh/ss1, site web sécurisé, diffusion de contenus via le réseau...)
- pour **signer** des documents électroniques
- pour **authentifier** des gens et des dispositifs
- pour vérifier l'**intégrité** d'un document
- ...

Les besoins en **intégration matérielle** sont aussi de plus en plus grands :

- pour les **performances** (vitesse, taille/poids, consommation d'énergie)
- pour la **sécurité** (éviter des attaques, le clonage, des modifications...)

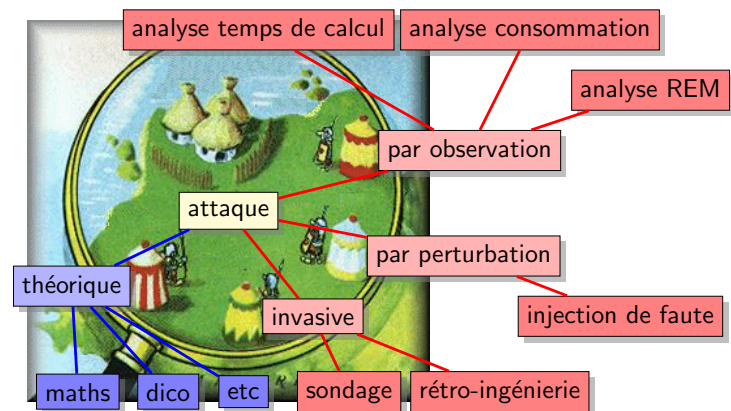
Exemple : chiffrement en crypto symétrique



Notations :

- \mathcal{M} message en clair
- $\mathcal{C} = \mathcal{E}_k(\mathcal{M})$ message chiffré
- \mathcal{E} algorithme de chiffrement
- \mathcal{D} algorithme de déchiffrement
- k clé secrète
- --- zone sécurisée
- --- canal de communication

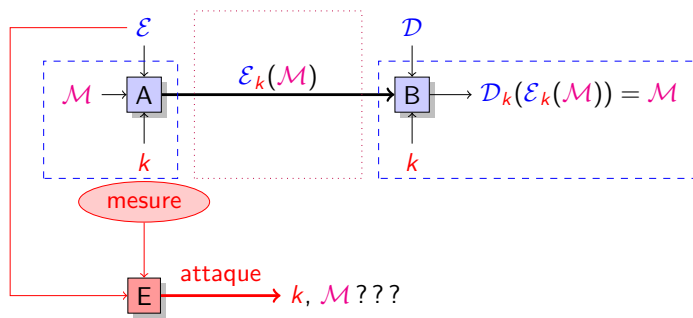
Quelques types d'attaques



REM = rayonnement électromagnétique

Attaque physique par canaux cachés

En anglais : *Side Channel Analysis/Attacks (SCA)*



Principe : mesurer des **paramètres externes** du dispositif pendant son fonctionnement pour en déduire des **informations internes**

Que mesurer ?

Réponse : **tout** ce qui peut "entrer" et/ou "sortir" dans le/du dispositif

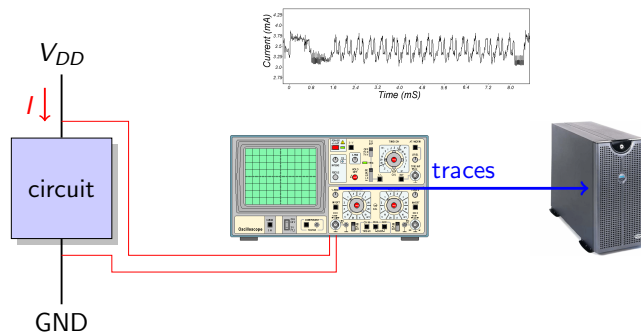
- la consommation d'énergie
- le rayonnement électromagnétique
- la température
- le bruit (son)
- le temps de calcul
- le nombre de défauts de cache
- le nombre et le type de messages d'erreur
- ...

Ce que l'on mesure peut donner des informations sur le comportement :

- **global** (température, consommation du circuit, bruit...)
- **local** (REM, nb défauts de cache...)

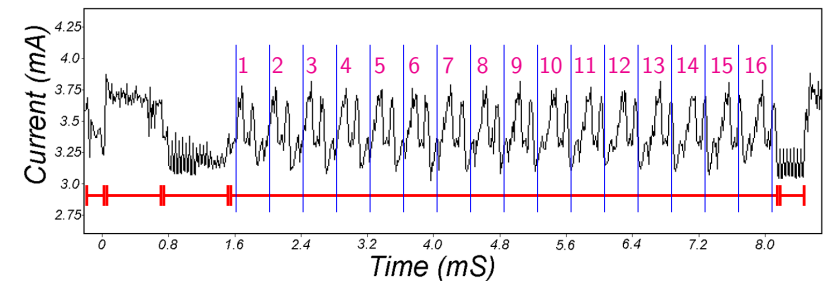
Attaque par mesure de la consommation d'énergie

Principe : mesurer le courant I qui alimente le dispositif



Notations : V_{DD} tension d'alimentation (5, 3, 2.5, 1.2 V), GND la masse

Que lire dans les traces ?



- Algorithmes \implies découpage en étapes
- Détection des tours de boucle (calculs répétitifs)
 - ▶ temps constant dans un tour
 - ▶ ou pas ???

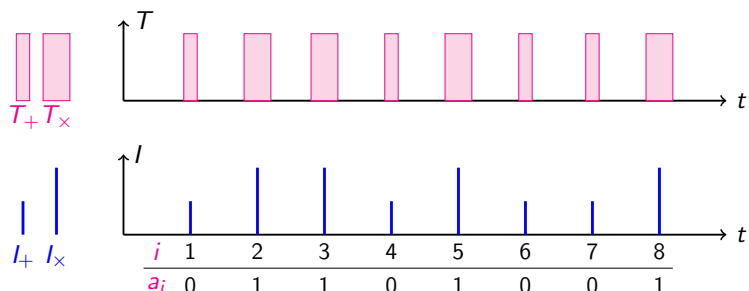
Exploiter les différences

Un algorithme a une **signature** en **courant** et en **temps de calcul** :

```

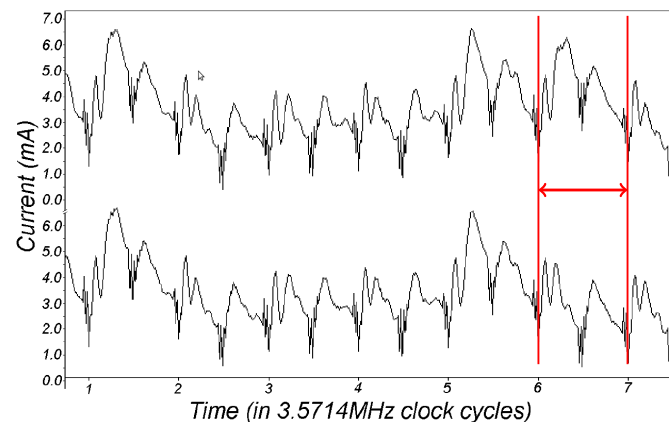
r = c0
for i from 1 to n do
  if ai = 0 then
    r = r + c1
  else
    r = r × c2

```



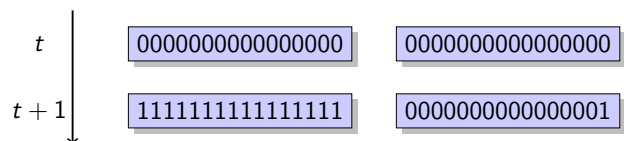
Analyse simple de la consommation (SPA)

En anglais : SPA *simple power analysis*



Limites de la SPA

Exemple de différence de comportement : (activité dans un registre)



Important : une petite variation de comportement peut être plus ou moins cachée par du **bruit** \implies les traces ne sont plus discernables

Question : que faire quand les différences sont (trop) petites ?

Réponse : utiliser des **statistiques** sur des **nombreuses** courbes

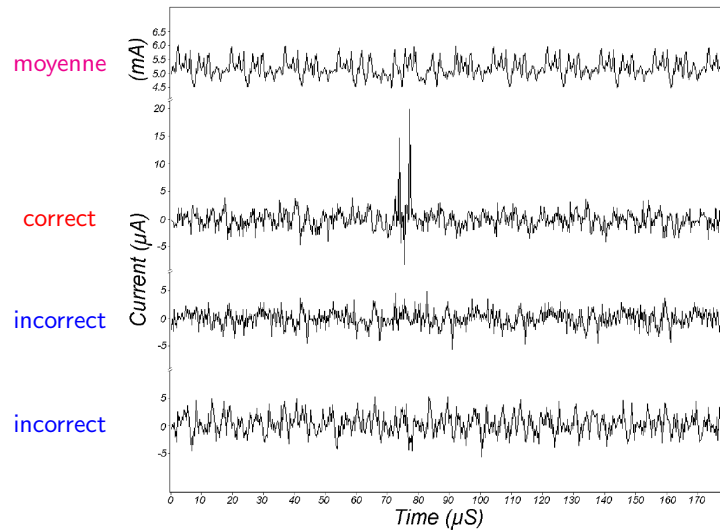
Analyse différentielle de la consommation (DPA)

En anglais : DPA *differential power analysis*

Principe :

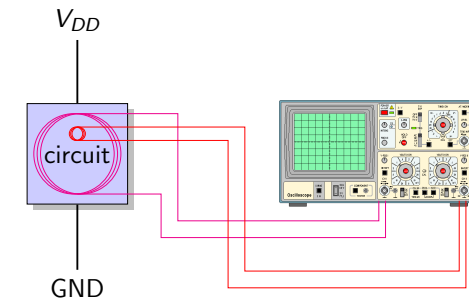
- effectuer N exécutions sur le crypto-système
 - on garde les messages en clair \mathcal{M}_i ($i \in \{1, \dots, N\}$)
 - on mesure les traces P_{ij} ($j \in \{1, \dots, T\}$)
- calculer la trace moyenne $\bar{P}_j = \frac{1}{N} \sum_{i=1}^N P_{ij}$
- sélectionner un bit b à attaquer (c.a.d. trouver b en interne)
- partitionner les traces P_{ij} en deux ensembles :
 - S_0 celles qui correspondent à $b = 0$ (tous les i qui donnent $b = 0$)
 - S_1 celles qui correspondent à $b = 1$ (tous les i qui donnent $b = 1$)
- faire une hypothèse sur b : $H = H_{b=0}$ ou $H_{b=1}$
- comparer statistiquement la trace moyenne globale \bar{P}_j à la trace moyenne de S_0 ou S_1 (celle de H)

Exemple de courbes obtenues par DPA



Analyse du rayonnement électromagnétique (1/2)

Principe : utiliser une sonde qui va capter le REM.



Mesure du REM :

- global avec une grande sonde
- local avec une microseconde

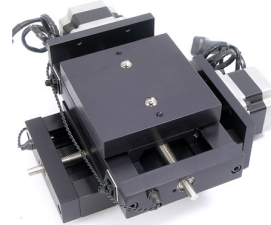
Analyse du rayonnement électromagnétique (2/2)

Contre-mesures

Types d'analyse du REM :

- simple : SEMA (*simple electromagnetic analysis*)
- différentielle : DEMA (*differential electromagnetic analysis*)

Le caractère local de l'analyse du REM peut être vraiment intéressant pour essayer de déterminer l'architecture du circuit, puis d'attaquer des endroits bien précis.



⇒ table X-Y

Empêcher une (ou des) attaques par :

- un nouveau dispositif de protection
- la modification/sécurisation du dispositif original

Exemples :

- blindage
- uniformiser les temps de calcul
- uniformiser la consommation d'énergie
- introduire du bruit (instructions inutiles)
- reconfigurer le circuit
 - ▶ changer le codage des données
 - ▶ changer les algorithmes
- ...

Addition modulo M

Entrées :

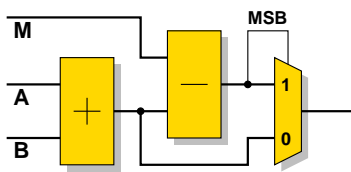
$$A, B \in \{0, 1, 2, 3, \dots, M - 1\}$$

Sortie¹ :

$$(A + B) \bmod M$$

Algorithme :

$$(A + B) \bmod M = \begin{cases} A + B & \text{si } A + B < M \\ A + B - M & \text{si } A + B \geq M \end{cases}$$



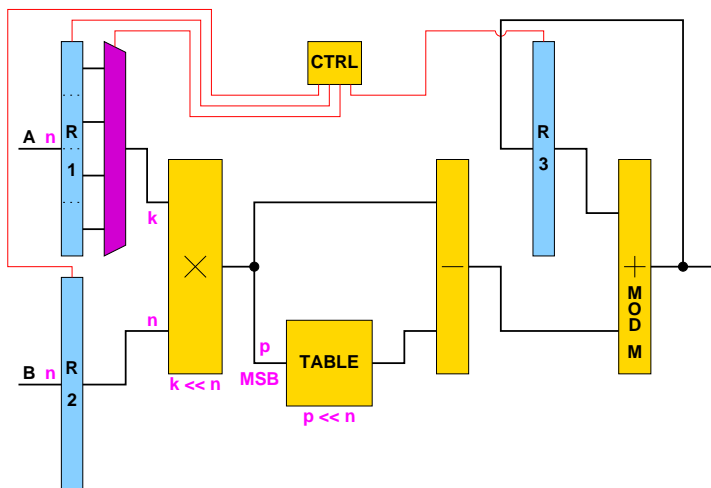
$$^1 0 \leq A + B \leq 2M - 2$$

Multiplication modulaire

Deux méthodes :

- multiplication **et** réduction modulaire
 - ▶ **étape 1** : calculer $P = A \times B$
 - ▶ **étape 2** : réduire $R = P \bmod M$
 - ▶ possible pour des M comme $2^n - 1$, $2^n + 1$ ou d'autres moduli spécifiques (mais pas en général)
- accumulation (modulaire) des **produits partiels réduits**
 - ▶ parallèle-parallèle
 - ▶ série-parallèle (MSB ou LSB en premier)

Multiplication modulaire : compromis



Exponentiation modulaire

Algorithme : *square and multiply*

Entrées : x , $d = (d_{m-1} \dots d_1 d_0)_2$
Sortie : $y = x^d$

```

1   $R \leftarrow 1$ 
2   $i \leftarrow m - 1$ 
3  while ( $i \geq 0$ ) do
4       $R \leftarrow R^2$            square
5      if ( $d_i = 1$ ) then
6           $R \leftarrow R \times x$    multiply
7      endif
8       $i \leftarrow i - 1$ 
9  endwhile
10 return  $R$ 
    
```

Opération majeure dans RSA

Double-Base Number Systems (DBNS)

Source : L. Imbert

Représentation **redondante** basée sur la somme de puissances de 2 et 3 :

$$x = \sum_{i=1}^n x_i 2^{a_i} 3^{b_i}, \text{ avec } x_i \in \{-1, 1\}, a_i, b_i \geq 0$$

Exemple : $127 = 108 + 16 + 3 = 72 + 54 + 1 = \dots$

	1	2	4	8	16
1					1
3	1				
9					
27			1		

	1	2	4	8
1	1			
3				
9				1
27		1		

Exemple : 127 a exactement 783 représentations DBNS, dont 6 sont canoniques : $127 = (108 + 18 + 1) = (108 + 16 + 3) = (96 + 27 + 4) = (72 + 54 + 1) = (64 + 54 + 9) = (64 + 36 + 27)$

Conclusion & perspectives

- **Attaques** de plus en plus **performantes**
- Sécurisation nécessaire à **tous les niveaux** (algo, opération, implantation)
- Sécurisation = compromis performances / robustesse
- Coût de sécurisation = $f(\text{valeur secret, type attaquant})$
- **Sécurité** = **informatique** + **micro-électronique** + **mathématiques**

Exemple de recherches actuelles :

- Exploiter les représentations redondantes
- Reconfiguration du circuit (représentations, algos)
- Rendre l'activité moins dépendante des valeurs
- Liens ordonnancement des sous calculs avec l'activité du circuit
- Exploration des compromis performances/robustesse

Représentations des chiffres au niveau circuit

Représentation classique d'un bit b :

- $V_{DD} \Rightarrow b = 1$
- $GND \Rightarrow b = 0$

_____ b

Représentation **double-rail** d'un bit b :

- $r_1 = V_{DD} \ r_0 = GND \Rightarrow b = 1$
- $r_1 = GND \ r_0 = V_{DD} \Rightarrow b = 0$

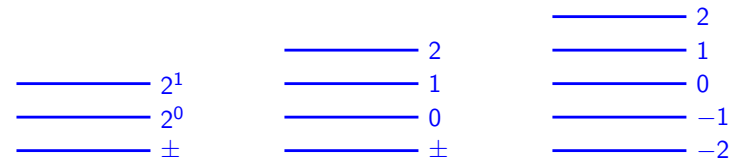
_____ r_1

_____ r_0

Intérêt : le nombre de transitions sur les fils (donc l'activité) est le même pour les transitions logiques $0 \rightarrow 1$ et $1 \rightarrow 0$

Coût : en surface de circuit et en mémoire

Codages en grande base : base 4 avec les chiffres $\{-2, -1, 0, 1, 2\}$



Fin, des questions ?

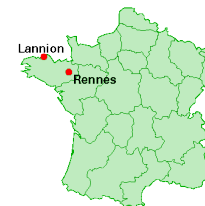
Contact:

- <mailto:arnaud.tisserand@irisa.fr>
- <http://www.irisa.fr/prive/Arnaud.Tisserand/>
- Equipe-projet CAIRN <http://www.irisa.fr/cairn/>
- Laboratoire IRISA, CNRS-ENSSAT-INRIA-Univ. Rennes 1
6 rue Kérampont, BP 80518, F-22305 Lannion cedex, France

Merci

ECOFAC 2010

<http://ecofac2010.irisa.fr>



- École thématique : **conception faible consommation pour les systèmes embarqués temps réel**
- 29 mars – 2 avril 2010, Plestin les Grèves, Côtes-d'Armor, Bretagne